Copyrighted Material

EFFECTIVE PHYSICAL SECURITY

Lawrence J. Fennelly

FOURTH EDITION

Copyrighted Material

Effective Physical Security

Fourth Edition

Lawrence J. Fennelly

ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Butterworth-Heinemann is an imprint of Elsevier

B
H

Acquiring Editor: MJ Peluso
Development Editor: Amber Hodge
Project Manager: Jessica Vaughan

Butterworth-Heinemann is an imprint of Elsevier
225 Wyman Street, Waltham, MA 02451, USA
The Boulevard, Langford Lane, Kidlington, Oxford, OX5 1GB, UK

Copyright © 2013 Elsevier Inc. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without permission in writing from the publisher. Details on how to seek permission, further information about the Publisher's permissions policies and our arrangements with organizations such as the Copyright Clearance Center and the Copyright Licensing Agency, can be found at our website: www.elsevier.com/permissions.

This book and the individual contributions contained in it are protected under copyright by the Publisher (other than as may be noted herein).

Notices
Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary. Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data
Application submitted

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

ISBN: 978-0-12-415892-4

Printed in the United States

For information on all BH publications visit our
website at www.elsevierdirect.com/security

12 13 14 15 16 10 9 8 7 6 5 4 3 2 1

Working together to grow
libraries in developing countries
www.elsevier.com | www.bookaid.org | www.sabre.org
ELSEVIER BOOK AID International Sabre Foundation

DEDICATION

I'm dedicating this book to my two lovely sisters, Christine and Sheila. Two totally different personalities, but very sweet and as loving as can be. I'm fortunate to have them as my sisters.

ACKNOWLEDGMENTS

It takes many hands and computers to write a book and this text is no exception. I'm deeply grateful to all those who over the years put down on paper their knowledge so others can benefit. I hope you realize how dedicated these individuals are to our profession. They spent countless hours at the computer creating their respective chapters.

My thanks to Mark Beaudry, PhD, CPP, who read the previous edition, page after page, noting corrections and deletions. Also, my thanks to Louis A. Tyska, CPP, and Donald Di Nardo; thank you for your advice and support. To Marianna Perry, MS, CPP; Randy Atlas PhD, CPP; Steve McKinnon, CPP; Joseph Nelson, CPP; Inge S. Black, CPP; Scott Fishman; and Rick Draper, who updated his paper after an operation in Australia.

Finally, my thanks to the staff at Elsevier. I'm privileged to work with such a dedicated group of individuals. I could not have completed this book without their professional assistance.

This book is intended for the practitioners who want to make a difference. Since 1980 when I compiled my first book, we have been doing research on what security practitioners need to know and what is new in the industry. One thing is very clear—things are changing rapidly. Physical assets protection systems need to be properly managed and most are not. Effective physical security is the use of devices to protect people, property, and information through proper management, inspection, and maintenance.

FOREWORD

When Larry Fennelly started out at the Harvard University Police Department more than 35 years ago (now retired), he knew nothing about crime prevention per se and knew less about physical security, procedural security, and assets protection until he attended the National Crime Prevention Institute at the University of Louisville, Kentucky. Plus, he got involved in ASIS and active with several councils. What were his goals? First, to be a good university police officer and to protect its assets (over 500 buildings) to which he had been assigned.

But he was also a visionary. He was able to identify the state of the art of loss/crime prevention in the 1980s and edited his first book, which is now in its fifth edition. He told me, "There was information that I needed and there wasn't a text around that had it, so we proposed and created the *Handbook of Loss Prevention*." To date, he has written/edited 29 books that are read by thousands and internationally accepted as well-known sources in the industry.

In those intervening years of change and development Larry learned and studied a lot about his profession. He progressed on the job and became a superior officer and later director of security for a museum at Harvard. He was a respected member in and out of his own campus enforcement environment. He obviously loves to write. I asked him who is/was his favorite security author. He replied "I have two: John Fay, CPP, and Norman Bottom, PHD, CPP, both trendsetters." I asked what he likes to read that is nonsecurity related, and he replied, "I have three favorites: W.E.B. Griffith, a genius with a typewriter and computer, Lee Child, and Michael Connolly; I can't get enough of them."

Much of what Larry has learned and experienced over the years is contained in his books. This text is not a conventional security book, as much of his practical personal experiences have influence over the many sections found within this effort. Contained in each chapter are the current necessary specifics to ensure that practitioners who have a need can reference this text with a particular and immediate dilemma and come up with a practical amount of knowledge to help solve the moment's crisis.

Overall this book contains the knowledge and experiences of about 40 professional security practitioners who have dozens of years of experience in the security field. This text as well as others will serve as one of the stages of development for your assets protection program.

Times have changed, and the world has changed its security level since September 11, 2001. What does that tell you? Simple: You must also advance with the times, think outside the box, and become a visionary as well.

Truly one of the hardest projects I have ever tackled is a recent project with Mark Beaudry, CPP, in which I edited his book *Security in the Year 2020*. I mention this because it's 2012, a period when we are into hybrid multichannel digital video recorders with digital deterrents, 1080p HD CCTV units, miniature color cameras with infrared LEDs, devices working with Iphones, robots, drones, 4G, and IP, all eco-friendly and low-energy consumption. So, I ask, are you ready for the future? Plan now!

Louis A. Tyska, CPP

CHAPTER

1

Influence of Physical Design

Marianna Perry, MS, CPP

INTRODUCTION

The relationship between physical design and informal social control of crime is a new idea only in the sense of its systematic application to the modern urban scene. Prior to the development of the modern city, most societies took some precautions to relate security in the physical environment to a responsibility for security actions by the inhabitants themselves.

In the rush of modern urban development, however, economic and political priorities seem to far outweigh security priorities, with the result that many urban settings now seem deliberately designed to discourage informal social control. No colonial community would have done so, even when stockades were no longer needed for defense. New England towns continued to be constructed so that homes and stores formed a hollow square around a central common area where social activities could take place and where livestock could be kept in relative security. In this kind of environment, everyone knew everyone else's business. While this meant less personal privacy than the modern city-dweller may enjoy, it also meant a high degree of shared responsibility for controlling undesirable behavior and unwanted intrusion.

Only recently have students of modern urban society begun again to take serious note of the relationship between physical design and informal social control. Jane Jacobs first applied the concept to modern cities in 1961. In her book *The Death and Life of Great American Cities* [1], she theorized that multiple land uses along residential streets provided an interaction between the physical design and the users (pedestrians and residents), which promoted natural and informal surveillance and, therefore, increased the safety of the streets.

Lee Rainwater, in an evaluation of a public housing project in St. Louis in 1966, discussed the effect of physical design on the attitudes of public housing residents, pointing out that inappropriate architectural design was directly related to antisocial behavior [2].

Elizabeth Wood, writing in 1961, suggested that current design patterns in public housing projects appeared to discourage informal social relationships and gatherings, thereby preventing the development of social interactions through which residents could create informal social controls and self-policing [3].

Schlomo Angel, in 1968, found that variations in the level of pedestrian and vehicular traffic could either encourage or discourage crimes [4]. Too few users provided enough potential victims, but not enough potential witnesses.

Gerald Leudtke and E. Lystad found, as the result of studies in Detroit, that

> *many of the features of urban form and structure…could tend to facilitate or decrease the4 probability of crime. Such physical features include the condition and maintenance of buildings, streets, and alleys; evidence of recent construction; mixtures of land use; rates of pedestrian traffic and pedestrian accumulation within various land uses; location of structures on an urban grid pattern; and distance to adjacent structures. Other examples are types of parking facilities; visibility into structures from roads, sidewalks and adjoining buildings; concealment by trees, shrubs, parked automobiles, fences, signs, and advertising; the visibility of entrance points; building setbacks; and, the number and arrangement of entrance points in a building [5].*

In 1969, Oscar Newman and George Rand [6] developed a theory of territoriality (now referred to as *defensible space*) that held that proper physical design of housing encourages residents to extend their social control from their homes and apartments out into the surrounding common areas. In this way, they change what previously had been perceived as semi-public or public territory into private territory. Upgrading the common areas in this way results in increased social control and an interaction between physical environment and its users that reduces crime.

As Newman himself defines it,

> *Defensible space is a surrogate term for the range of mechanisms—real and symbolic barriers, strongly defined areas of influence, improved opportunities for surveillance—that combine to bring an environment under the control of its residents. A defensible space is a living residential environment that can be employed by inhabitants for the enhancement of their lives, while providing security for their families, neighbors, and friends. The public areas of a multifamily residential environment devoid of defensible space can make the act of going from street to apartment equivalent to running the gauntlet. The fear and uncertainty generated by living in such an environment can slowly eat away and eventually destroy the security and sanctity of the apartment unit itself. On the other hand, by grouping dwelling units to reinforce association of mutual benefit, by delineating paths of movement, by defining areas of activity for particular users through their juxtaposition with internal living areas, and by providing for natural opportunities for visual surveillance, architects can create a clear understanding of the function of a space, who its users are and ought to be. This, in turn, can lead residents of all income levels to adopt extremely potent territorial attitudes and policing measures, which act as a strong deterrent to potential criminals [7].*

A study by Reppetto [8] in Boston indicated the need to expand the crime prevention through environmental design process to include whole neighborhoods and provide for comprehensive data collection efforts, which would both define the nature of crime patterns and suggest appropriate countermeasures.

Reppetto was also able to show that closely knit communities do tend to protect their members through informal social controls. This finding was further emphasized by John Conklin in *The Impact of Crime*:

> *A tightly knit community can minimize the problem of street crime. However, informal social control also poses a threat to the diversity of behavior that exists in a pluralistic society, even though it may curb violent crime. Still, street crime would decline if interaction among the residents of a community were more frequent, and if social bonds were stronger. A sense of responsibility for other citizens and for the community as a whole would increase individuals' willingness to report crime to the police and the likelihood of their intervention in a crime in progress. Greater willingness*

of community residents to report crime to the police might also obviate the need for civilian police patrols. More interaction in public places and human traffic on the sidewalks would increase surveillance of the places where people now fear to go. More intense social ties would reinforce surveillance with a willingness to take action against offenders [9].

C. Ray Jeffrey, in his classic theoretical work *Crime Prevention Through Environmental Design* (1971) [10], written before Jeffrey became aware of the works of Newman and others, proposed a three-fold strategy involving not only physical design, but also increased citizen participation and the more effective use of police forces. He contended that the way to prevent crime is to design the total environment in such a manner that the opportunity for crime is reduced or eliminated.

Jeffrey contends that both the physical and social characteristics of an urban area affect crime patterns. Better physical planning is a key to unlocking the potential for improved physical security and the potential for development of informal social control. He also argues for high levels of precision in the analytical stages that precede physical planning for crime reduction:

One of the major methodological defects in ecological studies of crime rates has been the use of large units and census tract data as a basis for analysis. The usual units are rural–urban, intricacy, intercity, regional, and national differences.…Such an approach is much too gross for finding the physical features associated with different types of crimes.

We must look at the physical environment in terms of each building, or each room of the building, or each floor of the building. Fine-grain resolution is required in place of the usual large-scale photographs.…Whenever crime rates are surveyed at a micro level of analysis, it is revealed that a small area of the city is responsible for a majority of the crimes. This fact is glossed over by gross statistical correlation analysis of census tract data, which ignore house-by-house or block-by-block variations in crime rates. For purposes of crime prevention we need data that will tell us what aspects of the urban environment are responsible for crime, such as the concentration of homicide or robbery in a very small section of the city [11].

DEFENSIBLE SPACE

Oscar Newman and others have explored and further defined the defensible space concept in recent years through design studies and experiments involving existing and new public housing projects. The following summary of defensible space techniques will give the practitioner an initial understanding of this important application of physical design to the urban residential environment.

Design for defensible space involves attempts to strengthen two basic kinds of social behavior called *territoriality* and *natural surveillance*.

Territoriality

The classic example of territoriality is the "a man's home is his castle" tradition of the American single-family home and its surroundings. In this tradition, the family lays claim to its own territory and acts to protect it. This image of the home as a castle reinforces itself "by the very act of its position on an integral piece of land buffered from neighbors and the public street by intervening grounds" [12].

As the urban setting has grown, the single-family home has become, to developers, an economic liability. Family housing has moved into the row house (townhouse), apartment complex, high-rise apartment structure, and massive public housing project. Whatever the benefits of this transition, the idea of territoriality has been largely lost in the process. The result is that "most families living in an apartment building

experience the space outside their apartment unit as distinctly public; in effect, they relegate responsibility for all activity outside the immediate confines of their apartment to the public authorities" [13].

As residents are forced by the physical design of their surroundings to abandon claim to any part of the outside world, the hallways, stairways, lobbies, grounds, parking lots, and streets become a kind of no-man's land in which criminals can operate almost at will. Public and private law enforcement agencies (formal controls) attempt to take up the slack, but without the essential informal social control that a well-developed social sense of territoriality brings, law enforcement can do little to reduce crime.

Natural Surveillance

The increased presence of human observers, which territoriality brings, can lead to higher levels of natural surveillance in all areas of residential space. However, the simple presence of increased numbers of potential observers is not enough, because natural surveillance, to be effective, must include an action component. The probability that an observer will act to report an observed crime or intervene in it depends on:

- The degree to which the observer feels that his or her personal or property rights are violated by the observed act.
- The extent to which the observer is able to identify with the victim or property under attack.
- The level of the observer's belief that his or her action can help, on the one hand, and not subject him or her to reprisals on the other.

Obviously, the probability for both observation and action is greatly improved by physical conditions, which create the highest possible levels of visibility.

Design Guidelines

Defensible space offers a series of architectural guidelines that can be used in the design of new urban residential complexes to promote both the residential group's territorial claim to its surroundings and its ability to conduct natural surveillance [14].

- **Site design** can stress the clustering of small numbers of residential units around private hallways, courtyards, and recreation areas. In these restricted zones, children can play, adults can relax, and strangers can easily be identified and questioned. Such private spaces can be created by internal and external building walls and access arrangements, and by the use of perceptual barriers such as a fence, shrubbery, and other boundary markers.
- **Site interrelationships design** can be used to create semi-private connecting and common spaces between and among the private family clusters. Walkways, vehicle access ways, parking areas, recreational facilities, lobbies, and laundry and shopping areas can be designed so that each cluster relates to them much like each resident of a cluster relates to his or her common private space. Physical design can be used to further extend the sense of territoriality and the possibility for informal social control.
- **Street design** and the design of other public spaces can be engineered to make these spaces into semi-public extensions of the residential clusters and their connectors. Closing streets to through traffic, installing benches and play areas near the streets, providing adequate lighting, and placing perceptual barriers to indicate the semi-public nature of the area can help to define these spaces as part of the shared residential group territory.
- **Surveillance-specific design** can be used in each of the design areas mentioned here to increase general visibility by providing adequate lighting, by reducing or eliminating physical barriers to visibility, and by the visibility-promoting location of key areas (e.g., entrances, lobbies, elevator waiting areas, recreational and parking areas) so as to be directly visible from as many viewpoints as possible.

Modifying Existing Physical Design

Cost limitations prevent substantial reconstruction of most existing urban residential facilities. However, a number of relatively low-cost techniques can be used to modify existing facilities so as to promote territoriality and natural surveillance. These include:

- Installing adequate security devices (locks, doors, and windows) in each residential unit.
- Dividing common lawn areas (front or back) into private yards and patios through the use of shrubbery, low fences, and other perceptual barriers.
- Improving the attractiveness and semi-privacy of pathways and other common outside areas by use of decorative paving and lighting: installing benches and other seating arrangements at strategic intervals, careful landscaping, and tying play areas, parking, and vehicle access ways to the overall design.
- Reducing the number of public access points and providing the remaining points with adequate lighting, visibility, and security.
- Establishing audio and video surveillance (monitored by residents or by security staff) in strategic internal areas.

It should be emphasized, in summary, that creating defensible space is not the same as creating a hardened security system (as might be found, for example, in a high-rise luxury apartment). In fact, it is almost the opposite: Defensible space operates on the premise that the living environment must be opened up and used by residents and others, not closed in. It is only in the open, used environment that people can be stimulated to establish the self-policing condition, which is informal social control. In this open living environment, opportunities for crime may continue to exist, but the probability for criminal activity is reduced.

It should also be emphasized that the physical design component of defensible space should always be accompanied by efforts to develop and sustain active citizen participation and by strategies for improved interaction between citizens and law enforcement agencies.

CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN

Crime prevention through environmental design (CPTED) is still a rapidly growing field of study and experimentation. CPTED attempts to apply physical design, citizen participation, and law enforcement strategies in a comprehensive, planned way to entire neighborhoods and major urban districts, as well as to specific urban subsystems such as public schools and transportation systems.

Cautions

Before summarizing the CPTED approach, we suggest that the practitioner view CPTED developments with a healthy skepticism, at least for the present. There are several reasons why a sense of caution is in order:

- CPTED approaches have been conclusively demonstrated.
- There is some disagreement among crime prevention theorists as to the correctness of the assumptions on which current CPTED programs are based.
- The magnitude of the typical CPTED project may be well beyond the practitioner's current ability to plan, implement, and manage.
- The cost of a typical CPTED project can represent a major financial investment, and unless the investment can be justified on a research and demonstration basis, there is no guarantee that it will be cost effective.

Despite these cautions, it is useful for the practitioner to be aware of the principles and current applications of the CPTED concept so that he or she can watch its developments and make appropriate use of the knowledge that it may produce.

Recent Projects

In a project combining the best of current community policing techniques with the principles of CPTED the city of Manchester, New Hampshire,

proved the value of this integrated approach. In Manchester, the police department formed partnerships with community organizations and provided appropriate crime prevention training, including CPTED to all of the officers assigned to the project areas. By combining the concepts of community policing with the application of CPTED, and other related crime prevention strategies, the community realized remarkable reductions in several crime categories. The area encompasses three areas of public housing in which CPTED principles were applied. The changes in community perceptions about crime were measured through surveys and the crime statistics were updated frequently to give the police department the best possible data. In this enterprise community area drug activity reduced 57%, robbery reduced 54%, burglary reduced 52%, and police calls for service dropped 20%. Additionally, the perceptions of the area's citizens were markedly improved. This example demonstrates the levels of success possible when sound policing, crime prevention, and the concepts of CPTED are combined in the correct proportions. As a result of these levels of success the project was recognized by the Department of Housing and Urban Development (HUD) through the awarding of the John J. Gunther Award. This award recognizes the best practices and was awarded in this instance in the category of Suitable Living Environment.

Territorial Defense Strategies. Territorial defense strategies emphasize prevention of property-related crimes such as breaking and entering, auto theft, and household larceny. Within this group there are five related strategy areas: land use planning, building grounds security, building perimeter security, building interior security, and construction standards.

- **Land use planning strategies** involve planning activities aimed at avoiding land use mixtures that have a negative impact on neighborhood security, through zoning ordinances and development plan reviews.
- **Building grounds security strategies** provide the first line of defense against unauthorized entry of sites and offer social control mechanisms to prevent dangerous and destructive behavior of visitors. The emphasis is on the access control and surveillance aspects of architectural design. The target environment might be a residential street, the side of a housing complex, or alleyways behind or between business establishments.
- **Building perimeter security strategies** provide a second line of defense for protecting site occupants and property by preventing unauthorized entries of buildings. They involve physical barriers, surveillance and intrusion detection systems, and social control mechanisms.
- **Building interior security strategies** provide the third line of defense for protecting site occupants and property by preventing unauthorized access to interior spaces and valuables through physical barriers, surveillance and intrusion detection systems, and social control mechanisms.
- **Construction standards strategies** involve building security codes that require construction techniques and materials that tend to reduce crime and safety hazards. These strategies deal both with code adoption and code enforcement.

It is important to be able to effectively evaluate territorial defense strategies and consider the three types of changes.

- Type one addresses design features such as locks, lights, fences, etc.
- Type two considers the impact of the implemented design features on the legitimate users of the property. Have they been inconvenienced by the changes in physical design and are they "on board" with in the risk management process?
- Type three changes deal with the direct effect of the intervening factors on crime and the indirect influence of physical design on crime [16].

Personal Defense Strategies. The second basic strategic approach focuses on the prevention of violent or street crimes such as robbery, assault, and rape, and the reduction of fear associated with these crimes. Specific strategies included safe streets for people, transportation, cash off the streets, and citizen intervention.

- **Safe streets for people strategies** involve planning principles derived primarily from the CPTED concepts of surveillance and activity support. Surveillance operates to discourage potential offenders because of the apparent risk of being seen and can be improved through various design modifications of physical elements of the street environment (e.g., lighting, fencing, and landscaping). Pedestrian traffic areas can be channeled to increase their use and the number of observers through such measures as creating malls, eliminating on-street parking, and providing centralized parking areas.
- **Transportation strategies** are aimed at reducing exposure to crime by improving public transportation. For example, transit waiting stations (bus, trolley) can be located near areas of safe activity and good surveillance, or the distance between stations can be reduced, which improves accessibility to specific residences, business establishments, and other traffic-generating points.
- **Cash off the streets strategies** reduce incentives for crime by urging people not to carry unnecessary cash and provide commercial services that minimize the need to carry cash.
- **Citizen intervention,** unlike the three previous strategies, consists of strategies aimed at organizing and mobilizing residents to adopt proprietary interests and assume responsibility for the maintenance of security.

Law Enforcement Strategies. The third general approach involves police functions that support community-based prevention activities. The two major activities are police patrol and citizen–police support.

- **Police patrol strategies** focus on ways in which police deployment procedures can improve their efficiency and effectiveness in responding to calls and apprehending offenders.
- **Citizen–police support strategies** consist of police operational support activities that improve citizen–police relations and encourage citizens to cooperate with the police in preventing and reporting incidents.

Community policing requires cooperation between members of the community and the police. Community members may be individual citizens, citizen groups, business associations, and government agencies and local offices that include health departments, building inspectors, and community development offices. Community members must be involved in not only calling the police to report a crime, but also helping to identify and solve other problems in the community. The most important element of community policing is problem solving, and crime is simply identified as a symptom of other problems in the community. The main focus of community policing is to deal with the underlying cause of crime and not just react to the symptoms of the problem [17].

Confidence Restoration Strategies. This fourth general strategy for commercial and residential environments involves activities that are aimed primarily at mobilizing neighborhood interest and support to implement needed CPTED changes. Without such interest and support, it is unlikely that programs of sufficient magnitude could possibly be successful, particularly in many high–crime rate neighborhoods where people have lost hope. There are two specific strategy areas: investor confidence and neighborhood identities.

- **Investor confidence strategies** promote economic investment and, therefore, social and economic vitality.
- **Neighborhood identity strategies** build community pride and foster social cohesion.

Most of these specific strategies are discussed in this and other chapters (some under different names). As a whole, this list of strategies is well organized and provides a good framework with which to view the possible interaction of a variety of crime prevention efforts.

Demonstrations. To see how these strategies were applied, let us look briefly at the major changes described in the American Architecture Foundation's presentation, *Back from the Brink: Saving America's Cities by Design* [18]. This provides examples of CPTED applications, with very little mention of crime, as applied in Portland, Oregon, and some other locales. The

principles applied are sound, workable redesign strategies that accomplish the goals of CPTED without overreliance on their direct crime prevention intent. Indeed, they are not presented as crime prevention, but redevelopment efforts, which consider the quality of life above most other considerations.

The CPTED applications in the featured cities achieve the following:

- Reduce opportunities for crime and fear of crime by making streets and open areas more easily observable, and by increasing activity in the neighborhood.
- Provide ways in which neighborhood residents, businesspeople, and police can work together more effectively to reduce opportunities and incentives for crime.
- Increase neighborhood identity, investor confidence, and social cohesion.
- Provide public information programs that help businesspeople and residents protect themselves from crime.
- Make the area more accessible by improving transportation services.
- Improve the effectiveness and efficiency of governmental operations.
- Encourage citizens to report crimes.

The steps taken to achieve these objectives include:

- Outdoor lighting, sidewalk, and landscaping improvements.
- Block watch, safe homes, and neighborhood cleanups.
- A campaign to discourage people from carrying cash.
- A major improvement and expansion of public transportation.
- Improved street lighting.
- Public transportation hubs that are purpose-built.

These improvements have enhanced the quality of life and provided an atmosphere of improvement in each of the communities featured.

The application of CPTED to school design has been promoted in a number of locations through the work of local practitioners, and in cooperation with school district personnel.

Additional CPTED case studies and information may be found in our text, written by Tim Crowe, *Crime Prevention through Environmental Design: Applications of Architectural Design and Space Management Concepts* [19]. This text offers CPTED as a specific topic and is widely used by students and practitioners.

The Future of CPTED

The most consistent finding in evaluations of CPTED and related projects is that the users of space must be involved in design decisions. Their involvement ensures that the designs are realistic and that the users will comply with the behavioral objectives of the plans. Numerous applications of CPTED concepts have been tried successfully on a spot basis, which tends to support the idea that the more simplistic approaches are the most viable. That is, it seems reasonable to assume that the crime prevention practitioner may confidently use CPTED strategies in very specific, controlled environmental settings.

There are many hundreds of examples of CPTED strategies in practice today. It is unfortunate that most of the successful applications have not been publicized well, since they are usually part of ongoing field activities that do not come to the attention of evaluators or government agencies. However, it has been noted that most applications center on some mixture or interaction between the three basic CPTED processes of natural surveillance, natural access control, and territoriality. The most basic common thread is the primary emphasis on naturalness—simply doing things that you already have to do, a little better.

The most productive uses of CPTED, in the foreseeable future, will center on the following simplistic strategies:

- Provide clear border definition of controlled space.
- Provide clearly marked transitional zones that indicate movement from public to semi-public to private space.

- Relocate gathering areas to locations with natural surveillance and access control, or to locations away from the view of would-be offenders.
- Place safe activities in unsafe locations to bring along the natural surveillance of these activities (to increase the perception of safety for normal users and risk for offenders).
- Place unsafe activities in safe spots to overcome the vulnerability of these activities with the natural surveillance and access control of the safe area.
- Redesignate the use of space to provide natural barriers to conflicting activities.
- Improve scheduling of space to allow for effective use, appropriate "critical intensity," and the temporal definition of accepted behaviors.
- Redesign or revamp space to increase the perception or reality of natural surveillance.
- Overcome distance and isolation through improved communication and design efficiencies.

The future of CPTED rests with the persons who shape public and private policy. Crime prevention practitioners will have to communicate CPTED concepts in terms that relate to the overall priorities of their organizations or communities. Productivity, profitability, and quality of life are concerns that affect policymakers, not specifically security or crime prevention for its own sake. Accordingly, chief executives, builders, architects, planners, engineers, and developers will have to embrace CPTED design objectives. Elected officials and legislative bodies will have to be held accountable for assuring that CPTED is considered in capital improvement and development plans. Property owners and residents of neighborhoods and commercial areas need the opportunity to question planning, zoning, and traffic signalization decisions. Finally, strategic plans that encompass 20-year community development periods require an assessment of crime prevention needs and programs.

The United States federal government initiated physical design criteria to ensure appropriate protection for federal buildings and occupants after the 2001 terrorist attacks at the World Trade Center and the Pentagon and the 1995 bombing of the Murrah Federal Building in Oklahoma. These guidelines take into account not only physical security but also CPTED.

CONCLUSION

The application of environmental design concepts by the crime prevention practitioner can be as cost effective as the design of crime risk management systems for individual place managers. Such an application must be based, however, on sound analysis of particular crime patterns and the physical and social conditions that are related to those patterns. It should stress innovative solutions that are appropriate to the particular circumstances, that are cost effective, and that will not create more problems than they solve. It should stress working with "things as they are" rather than with "things as they ought to be."

The practitioner needs, above all, to become well acquainted with the people and organizations responsible for physical development and redevelopment in his or her community. The best opportunities for applying crime prevention through environmental design occur when buildings, street layouts, street lighting programs, new subdivisions, shopping centers, and housing projects are still in the planning stages, and crime prevention principles can be incorporated before construction starts. Good security design can help prevent crime. It is important to remember that the premise behind CPTED is the physical design and the use of space. It is not the typical target-hardening approach to crime prevention [20].

In keeping with the theory that the quality of the physical environment impacts human behavior, we think that crime prevention and community development go hand in hand. Physical design that enhances the environment from a balanced economic–social–political standpoint can also discourage criminal activity, and the concept of crime prevention through environmental design can be used in any situation—high-density urban areas, small cities and towns, and even rural areas. The essential role of the practitioner

is to see the "whole picture" and to see to it that physical design, citizen participation, and police activities fit together.

In June 2009, ASIS International published a guideline entitled "Facilities Physical Security Measures, ASIS GDL, FPSM-2009" [21]. This publication includes CPTED along with typical physical security countermeasures as a major component in any crime prevention program. The physical design of an environment is an important element to consider and the major task of the crime prevention practitioner is to analyze existing and planned physical design, to determine how it relates to existing or potential crime patterns, and recommend physical design countermeasures to the proper person or organization.

REFERENCES

[1] Jacobs J. The death and life of great American cities. New York: Vintage Books; 1961.
[2] Rainwater L. Fear and the home-as-haven in the lower class. Journal of the American Institute of Planners, January 1966:23–37.
[3] Wood E. Housing design: A social theory. New York: Citizens' Housing and Planning Counsel of New York, Inc; 1961.
[4] Angel S. Discouraging crime through city planning. Berkeley: University of California Press; 1968.
[5] Leudtke G, Lystad E. Crime in the physical city. Final Report. LEAA Grant No. NI 1970:69–78.
[6] Newman O, Rand G. Defensible space. Published by Oscar Newman. New York Publishing: Macmillan; 1972.
[7] National Institute of Law Enforcement and Criminal Justice, 1972. Urban design, security, and crime. Proceedings of a seminar held April 12–13, 1972, published by the Law Enforcement Assistance Administration (LEAA), p. 15.
[8] Reppetto TA. Residential crime. Cambridge, MA: Ballinger Publishing; 1974.
[9] Conklin J. The impact of crime. New York: Macmillan Publishing; 1975, 299.
[10] Jeffrey CR. Crime prevention through environmental design. Beerly Hills, CA: Sage Publications; 1971.
[11] Jeffrey CR. Behavior control techniques and criminology: 1975. Ecology Youth Development Workshop. Honolulu: University of Hawaii School of Social Work; 1975.
[12] Op. cit., Newman, pp. 51–52.
[13] Ibid.
[14] Ibid.
[15] Newman O. Design guidelines for creating defensible space. Washington, DC: LEAA; 1976.
[16] Robidas, RL, 1996. Reports on activity in project area for the Manchester (NH) police department.
[17] Lab SP. Crime prevention: Approaches, practices and evaluations. Bowling Green State University, OH: Anderson Publishing; 2007.
[18] American Architecture Foundation. Back from the brink: Saving America's cities by design, videocassette. American Architecture Foundation 1996, Washington DC.
[19] Crowe TD. Crime prevention through environmental design: Applications of architectural design and space management concepts. Stoneham, MA: Butterworth; 1991.
[20] Atlas RI. 21st century security and CPTED. Boca Raton, FL: Auerbach Publications; 2008.
[21] ASIS International. Facilities physical security measures guideline. Alexandria, VA: ASIS International; 2009, ASIS GDL, FPSM-2009.

CHAPTER

2

Introduction to Vulnerability Assessment*

Mary Lynn Garcia

This text is a follow-on to the previously published *Design and Evaluation of Physical Protection Systems*. That book (hereafter referred to as the *Design* textbook) provided an overview of the principles and concepts that must be considered when implementing a physical protection system (PPS); this book is a description of how to apply those principles and concepts to identify the vulnerabilities of an installed PPS and propose effective upgrades if needed. This book is the basis of all vulnerability assessments (VAs) conducted by Sandia National Laboratories during the last 30 years for a wide spectrum of customers including the U.S. Department of Energy, U.S. Department of Defense, North Atlantic Treaty Organization, U.S. Department of State, Government Services Administration, dam and water systems, prisons, schools, communities, and chemical companies.

A VA is a systematic evaluation in which quantitative or qualitative techniques are used to predict PPS component performance and overall system effectiveness by identifying exploitable weaknesses in asset protection for a defined threat. After the VA identifies weaknesses, it is used to establish the requirements for an upgraded PPS design. In addition, a VA is also used to support management decisions regarding protection system upgrades. Risk assessment and VA are such closely related activities that many security professionals use the terms interchangeably. This may not present a huge problem in practice, but it does hinder communication between and among security service providers and customers.

The VA process can be broken into three distinct phases: planning, conducting the VA, and reporting and using the results. This process is part of the larger risk assessment process. Each of the phases will be described in detail in the remaining chapters of this text. The key points discussed in this chapter include:

- Risk management and vulnerability assessment
- Risk assessment and the vulnerability assessment process
- Vulnerability assessment process overview
- Vulnerability assessment and systems engineering

This text is concerned with the VA of a PPS, but the concepts can be applied to cyber protection, personnel protection, and overall security protection at a facility or across an enterprise. For clarity, throughout this text the term enterprise includes organizations, companies, agencies,

*Originally from Garcia, ML. Vulnerability assessment of physical protection systems. Boston: Butterworth-Heinemann, 2006. Updated by the editor, Elsevier, 2011.

governments, or any other entity with the need to manage security risks. The term asset includes people, property, information, or any other possession of an enterprise that has value.

It is important to differentiate security from safety when discussing a VA. Safety is defined as the measures (people, procedures, or equipment) used to prevent or detect an abnormal condition that can endanger people, property, or the enterprise. These include accidents caused by human carelessness, inattentiveness, and lack of training or other unintentional events. Security, on the other hand, includes the measures used to protect people, property, or the enterprise from malevolent human threats. This includes civil disturbances, sabotage, pilferage, theft of critical property or information, workplace violence, extortion, or other intentional attacks on assets by a human. A good security VA will consider safety controls because some safety measures aid in detection and response to security events (sprinklers will fight fires regardless of the cause), but some attacks require additional detection and response capability. For example, a disgruntled employee can sabotage critical manufacturing equipment and reduce production to a significant extent. Without security controls, it could be difficult to determine quickly enough whether this is an intentional act of sabotage and prevent a significant loss of revenue.

RISK MANAGEMENT AND VULNERABILITY ASSESSMENT

Risk management is the set of actions an enterprise takes to address identified risks and includes avoidance, reduction, spreading, transfer, elimination, and acceptance options. Good risk management programs will likely include a combination of these options. Risk avoidance is accomplished by removing the source of the risk; for example, a company may choose to buy a critical component from another company, rather than manufacture it. This removes the production line as a sabotage target. Risk reduction is achieved by taking some actions to lower risk to the enterprise to reduce the severity of the loss. This is the goal of many security programs—lower risk by implementing at least some security measures. Risk can also be spread among multiple locations, perhaps by having similar production capability at more than one enterprise facility. Then, loss of capability at one site may be managed by increasing production at the other locations. Another example of risk spreading is the distribution of assets across a large industrial facility. By separating the assets, fewer assets may be at risk during any given adversary attack. Risk transfer is the use of insurance to cover the replacement or other costs incurred as a result of the loss. This is an important tool in many security systems. Risk acceptance is the recognition that there will always be some residual risk. The key is to knowingly determine an acceptable level, rather than unwittingly accepting it. In security risk management, these decisions are based on the consequence of loss of the asset, the defined threat, and the risk tolerance of the enterprise. A trade-off analysis must be performed to ensure that the dollars spent on physical security provide a cost-effective solution to security issues. If other risk management options provide equal or better results at lower cost, the use of a PPS may not be justified.

Security is only one facet of risk; therefore, it must be considered in the context of holistic risk management across the enterprise, along with other categories such as market, credit, operational, strategic, liquidity, and hazard risks. The relationships among risk management, risk assessment, and vulnerability assessment are shown in Figure 2-1. Risks across an enterprise must be managed holistically, and those identified as above an acceptable level must be addressed. VA is one of the constituent pieces of security risk assessment and is used to support risk management decisions.

To frame the relationship between risk assessment and risk management, consider definitions provided by Kaplan and Garrick, who state that in risk assessment, the analyst attempts to answer the three questions: What can go wrong?

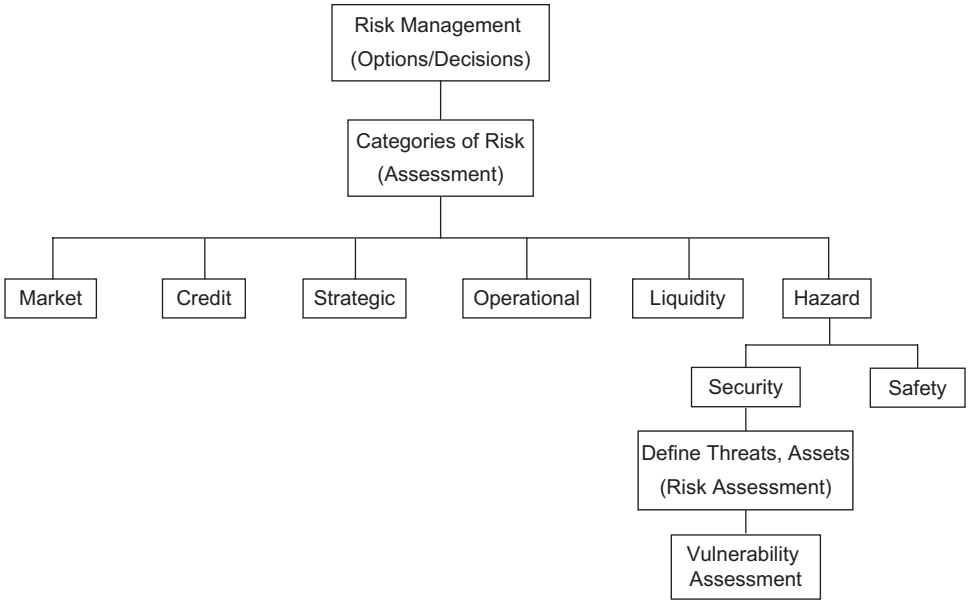


FIGURE 2-1 Relationship between risk management and vulnerability assessment.

What is the likelihood that it would go wrong? What are the consequences? The answers to these questions help identify, measure, quantify, and evaluate risks. Then, risk management builds on risk assessment by answering a second set of questions: What can be done? What options are available? What are their associated trade-offs in terms of costs, benefits, and risks? What are the impacts of current management decisions on future options? The answer to the last question provides the optimal solution. Total risk management results from this process, where total risk management is defined as a systematic, statistically based, holistic process that builds on formal risk assessment and management by answering the two sets of questions and addressing the sources of system failures.

A security risk assessment is the process of answering the first three questions using threat, likelihood of attack, and consequence of loss as their benchmarks.

A thorough security risk assessment would consider risks in the component parts of a security system (cyber, executive, transportation protection, etc.) to facilitate informed risk decisions across the enterprise. As applied to the VA of a PPS, risk assessment is an evaluation of the PPS supported by a number of analysis methodologies, including:

- Threat analysis
- Consequence analysis
- Event and fault tree analyses
- Vulnerability analysis

RISK ASSESSMENT AND THE VULNERABILITY ASSESSMENT PROCESS

Most facilities or enterprises routinely conduct risk assessments of their security systems to verify that they are protecting corporate assets and to identify areas that may need additional attention. These assessments are defined differently for different enterprises, but in general they include consideration of the likelihood of a negative event; in this case it is a security incident and the consequence of that event. The *Design* textbook ended with a description of risk assessment and provided a formula that can be used

to calculate risk, using qualitative or quantitative measures. That discussion, with one addition, is repeated here.

Security risk can be measured qualitatively or quantitatively through the use of the following equation:

$$R = P_A \times (1 - P_E) \times C$$

where

R = risk to the facility (or stakeholders) of an adversary gaining access to, or stealing, critical assets. Range is 0–1, with 0 being no risk and 1 being maximum risk. Risk is calculated for a period of time, such as 1 year or 5 years.

P_A = probability of an adversary attack during a period of time. This can be difficult to determine, but generally there are records available to assist in this effort. This probability ranges from 0 (no chance at all of an attack) to 1 (certainty of attack). Sometimes in the calculation of risk, we assume there will be an attack, which mathematically sets $P_A = 1$. This is called a conditional risk, where the condition is that the adversary attacks. This does not mean there will absolutely be an attack, but that the probability of attack is unknown or the asset is so valuable that it will be protected anyway. This approach can be used for any asset, but it is generally reserved for the most critical assets of a facility, where the consequence of loss is unacceptably high, even if P_A is low. For these assets, a PPS is generally required.

$P_E = P_I \times P_N$, where P_I is the probability of interruption by responders, and P_N is the probability of neutralization of the adversary, given interruption. P_N can include a range of tactics from verbal commands up through deadly force. The appropriate response depends on the defined threat and consequence of loss of the asset. P_E represents the vulnerability of the PPS to the defined threat.

C = consequence value, or a value from 0 to 1 that relates to the severity of the occurrence of the event. This is a normalizing factor, which allows the conditional risk value to be compared to other risks across the facility. A consequence table of all events can be created that covers the loss spectrum, from highest to lowest. By using this consequence table, risk can be normalized over all possible events. Then, limited PPS resources can be appropriately allocated to ensure that the highest consequence assets are protected and meet an acceptable risk.

Note that this equation introduces the use of a new term—the *probability of neutralization* (P_N). This was discussed only briefly in the *Design* book, because many facilities do not have an immediate response to security events. It is included here because response is a part of VA at all facilities.

Using probabilistic risk assessment is more formal, scientific, technical, quantitative, and objective when compared to risk management, which involves value judgment and heuristics and is more subjective, qualitative, societal, and political. Ideally, the use of probabilities is based on objective likelihoods, but in security it is common to use more subjective likelihoods based on intuition, expertise, partial, defective, or erroneous data and occasionally, dubious theories. This is important because these are major sources of uncertainty, and uncertainty is a major element of risk. Additionally, these measures can reduce the credibility of the security risk assessment for senior management, who are used to seeing documented data in standard analysis models. In security systems, this uncertainty is even larger than normal, owing to the lack of dependable (i.e., quantifiable) data for all types of adversary attacks.

An additional use of the risk equation is that the security risk life cycle can be viewed in context. When considering security systems and the attack time line, the attack can be broken into three discrete phases: pre-attack, which is the time the adversary takes to plan the attack; the attack phase, when the adversary actually shows up to attack the facility, and the attack has started; and post-attack, when the adversary has completed the attack, and the consequences of a successful attack occur. If the problem is

approached this way, each term in the equation is of primary importance during different phases of the attack. As such, P_A is most useful during the pre-attack phase. This is where intelligence agencies and deterrence have their biggest effect. Intelligence agencies gather information concerning threats and provide assessments about their likelihood of attack. These agencies may even develop enough information to disrupt an attack by collecting enough legal evidence to arrest the adversary, through tips from inside sources, or by alerting targeted enterprises, allowing them to increase security protection. All of these activities will have an effect on P_A. Heightened security responses to intelligence assessments indicating potential attacks on Citibank and the stock exchange in New York, and the World Bank in Washington, DC, are recent examples of pre-attack influences.

If a quantitative approach is used, the P_A and C terms can be calculated using historical data and consequence criteria, respectively. In a qualitative analysis, these terms can be represented using descriptors such as likely, very likely, or not likely for P_A and critical, severe, or minimal for the C term. This determination is based on the capability of the threat and the consequence of loss of the asset. If the likelihood of attack is high, but the consequence is low (think about shoplifting at one store in an enterprise), the problem to be solved is easier than if both P_A and C are high. (This ignores the cumulative effects of shoplifting across the enterprise. Many thefts of low-value items can add up to a high overall impact and this is part of the analysis.) There are times when either approach is appropriate, and the choice should be driven by the consequence of loss. This is based on the assumption that assets with a higher consequence of loss will attract more capable and motivated adversaries (threats), which in turn will require a PPS that is correspondingly more effective. Figure 2-2 represents the transition from qualitative to quantitative analysis, using consequence as the discriminator. Qualitative analysis uses the presence of PPS components and adherence to PPS principles as system effectiveness measures. A quantitative analysis uses specific component performance measures derived from rigorous testing to predict overall system effectiveness. At any given facility either or both techniques may be used depending on the consequence of loss of the asset. Relative value of PPS components based on expert opinion is another form of analysis of system effectiveness; however, the outcome depends heavily on the knowledge and experience of the expert.

This section ends with a definition of terms that are used in risk assessments, particularly with respect to the probability of attack by an

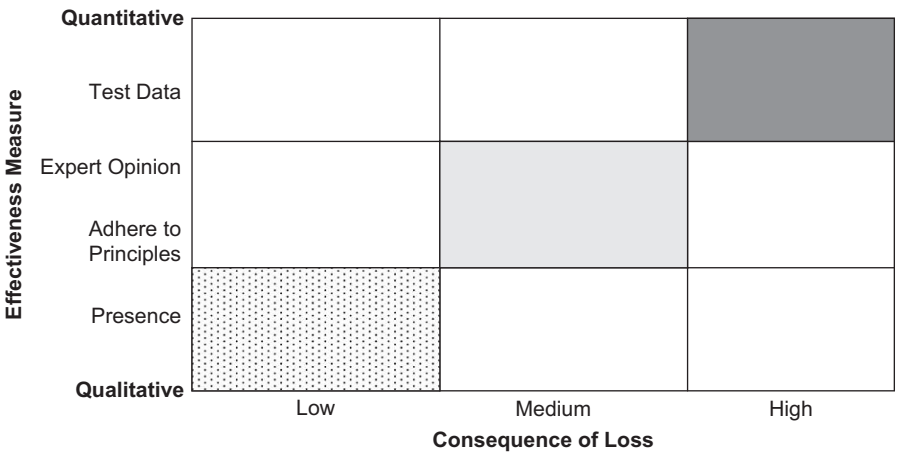


FIGURE 2-2 Application of qualitative and quantitative analysis approaches.

adversary. These are the proper definitions of these terms; some enterprises may use them differently. Probability is a number that is, by definition, between 0 and 1, and may or may not be time dependent. (As an example, the probability of snow on any given day in Ohio may be 0.25, but the probability of snow in Ohio is 1.0 over the next year.)

This is discussed further in the next section. Although probability of attack is routinely cited as a threat measure, it is important to note that there frequently is not enough data to support a true probability. For example, there is no statistical data to support the probability of terrorist attacks. That fact, however, has not prevented the massive expenditure of dollars by governments and commercial enterprises to increase security at airports, seaports, critical infrastructures, and other facilities since 9/11. This is a good example of high-consequence, low-probability events and the use of conditional risk. For some assets, the consequence of loss is unacceptably high, and measures are taken to prevent successful adversary attacks, regardless of the low likelihood of attack. Frequency refers to how many times an event has happened over a specified time and is also called a rate. Annual loss exposure is an example of a frequency often used in security risk assessments. Likelihood may be a frequency, probability, or qualitative measure of occurrence. This is more of a catch-all term and generally implies a less rigorous treatment of the measure. Haimes has written a thorough discussion of risk modeling, assessment, and management techniques that can be used in security or general risk applications.

STATISTICS AND QUANTITATIVE ANALYSIS

In any discussion of quantitative security system effectiveness, the subject of statistics of security performance arises. To many, statistics is a subject that arouses suspicion and even dread; however, there are a few fairly simple concepts that form the basis of statistical analysis of security effectiveness. Most of these concepts are related to the possible outcomes of a security event. A security event occurs when a security component (people, procedures, or equipment) encounters a stimulus and performs its intended task, for example, when something, such as a human or small animal, enters the detection envelope of an intrusion sensor. There are four possible outcomes of this event:

1. The sensor successfully detects a human-size object.
2. The sensor fails to detect a human-size object.
3. The sensor successfully ignores a smaller-than-human-size object.
4. The sensor fails to ignore a smaller-than-human-size object.

The successes and failures are related such that when a human-size object is presented, there are two complementary results, and when a smaller-than-human-size object is presented, there are also two complementary results. This fact is used later in the discussion. Sensors are the example used here, but this principle applies to any of the probabilities used in this text—the success or failure of a PPS component or the system in performing its intended task can be measured.

Most statistical analysis of security performance is based on these four possible outcomes. The rate at which a sensor successfully detects objects is described as the detection rate. For example, if a sensor successfully detects a human-size object 9 times out of 10 events the detection rate for that group of 10 events is 0.9 or 90%. This is a statistic but is not yet a probability. The detection rate can be turned into a probability when coupled with a confidence level, which is established based on the number of events that are analyzed; the more data available, the more confidence there is in the probability. This is easily understood when considering a common example. If a person tosses a coin and the outcome is heads, it would be unwise to assume that every coin toss will result in heads. However, if that person tosses a coin 100 times and 49 results are heads and 51 results are tails, there is a fairly

high confidence that the outcomes will be about 50/50. If the experiment is continued to include 1,000 trials, the confidence in the estimate of the likely results is even higher. At this point the rate can be estimated with some statistical confidence, and this estimate is a probability. In other words, a probability is an estimate of predicted outcomes of identical trials stated with a confidence level. If 100% confidence is required, an infinite number of tests are required. In reality, when designing performance tests, a confidence level is chosen that requires performance of a reasonable number of trials.

It is not the intent of this section to teach readers how to calculate the statistics of security component effectiveness, but to familiarize them with the terminology and underlying concepts as applied to a PPS. For example, if a metal detector is tested by carrying a gun through it 20 times and it detects all 20 times, the probability of detection can be calculated at a specified confidence level. Often the confidence level used for security component testing is 95%. Using this confidence level, the probability calculated for the metal detector based on the 20 trials is 0.85 (it is often said that the probability is 85%, but in proper statistical terminology a probability is always a number between 0 and 1). In simpler language, there is a 95% confidence that the metal detector will detect the gun at least 85% of the time. The actual detection rate may be higher, but this is what can be supported given the amount of data collected. If the metal detector is tested 30 times at the same 95% confidence, the probability is now 0.9. Again restating in simple language, there is a 95% confidence that the metal detector will detect the gun at least 90% of the time.

Sometimes it is more useful to classify PPS component performance into error rates rather than probabilities. These error rates are the mathematical complement of the success rates, which is the number of trials minus the number of successes (i.e., the number of failures). The error rates are stated as false accept and false reject rates. In the preceding sensor example, not detecting the human-size object is a false accept and detecting a smaller-than-human-size object is a false reject. This example is used to show that these are the same possible outcomes; however, error rates are seldom used when describing the performance of detection sensor devices. Error rates are much more useful when characterizing the performance of entry control devices, particularly when evaluating the performance of biometric identity verification devices. These devices measure some biological feature, such as a fingerprint, to verify the identity of an individual. In this case, false acceptance of a fingerprint from someone who should not be allowed into a security area and false rejection of someone who should be allowed to enter a secured area are useful ways to view the data.

Other factors of interest in security component evaluation include discrimination and susceptibility to noise. Discrimination describes a sensor's ability to ignore an object that is of the appropriate magnitude but is not the intended target. Often, this is beyond the technical capability of the device. In the preceding sensor example, a human-size object may or may not have specific characteristics that allow the sensor to discriminate between a human and a human-size animal like a small deer or large dog. When the sensor does not have the ability to discriminate between stimuli of equal magnitude, another statistic, the nuisance alarm rate, is used. A nuisance alarm is caused when the sensor detects an object that is of sufficient magnitude but benign in nature. Anyone who has had a belt buckle cause an alarm in an airport metal detector has experienced a nuisance alarm (assuming that person was not also carrying a gun!). The sources of nuisance alarms are easy to identify when the alarm is assessed by direct human observation or by viewing an image using a video camera. Understanding the causes of nuisance alarms is important in both design and analysis of a PPS. Installing a sensor that has low discrimination to an object or condition that is continually present in the sensor's operating environment will lead to a high nuisance alarm rate, thus lowering confidence in the system. In this scenario, human operators eventually discount alarms and may

not pay sufficient attention to a real alarm when it occurs.

Some technologies are also susceptible to noise. Noise in the sensor includes sound, electromagnetic, or even chemical sources. This noise can be present in the background or internal to the system. Whenever a sensor alarms on external or internal noise, this is defined as a false alarm. False alarms also reduce system effectiveness much the same way as nuisance alarms. Indeed, false alarms can further erode confidence in the PPS because there is no observable alarm source present.

Throughout the discussions of security component performance in this text, it is important to remember that the four possible outcomes of any event are considered. This information, together with the concepts of discrimination and susceptibility to noise, form the basis of almost all security component performance evaluation. Combined with defeat analysis (which is discussed in other chapters), the full picture of PPS effectiveness emerges.

VULNERABILITY ASSESSMENT PROCESS OVERVIEW

The evaluation techniques presented in this text use a system performance-based approach to meeting the PPS objectives. Recall that the primary functions of a PPS are detection, delay, and response (see Figure 2-3). Each of these functional subsystems is described in the following chapters and includes a description of both quantitative and qualitative methods of evaluating PPS components at a facility. Quantitative techniques are recommended for facilities with high-consequence loss assets; qualitative techniques can be used if there is no quantitative data available or if the asset value is much lower. It is important to determine before the start of the VA whether a qualitative or quantitative analysis technique will be used. This ensures that the VA team collects the appropriate data and reports their results in a form that is useful for the analysis.

When performing a VA, the general purpose is to evaluate each component of the PPS

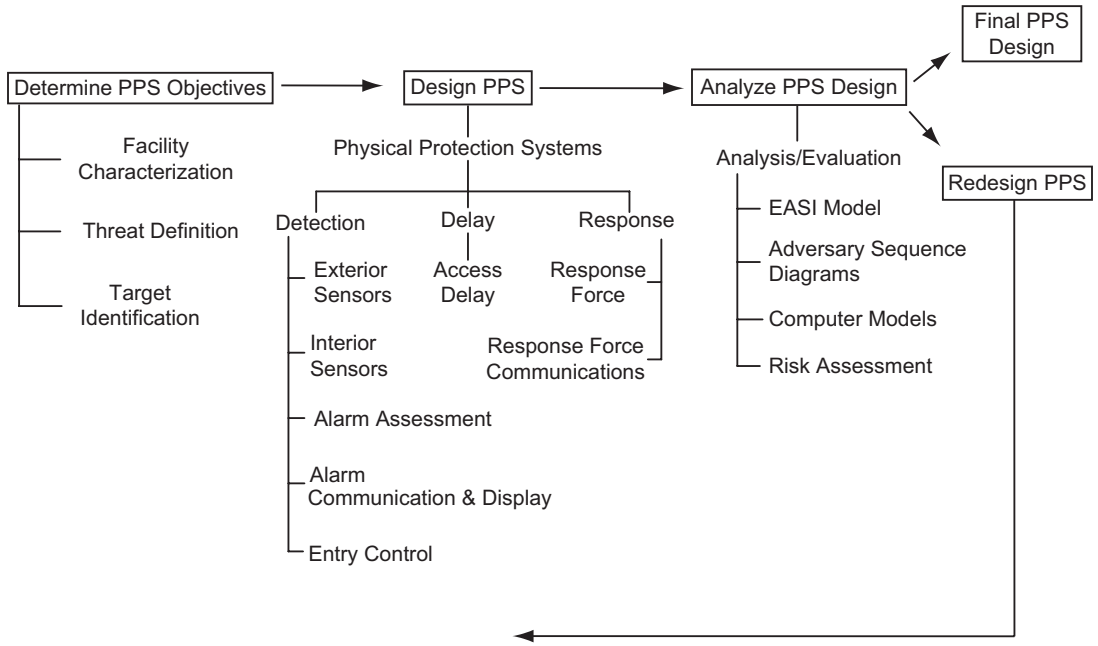


FIGURE 2-3 PPS evaluation process. As in the *Design* textbook, this process provides the framework for conducting a vulnerability assessment. Although frequently not part of the VA, the protection objectives must be known before evaluating the facility.

to estimate their performance as installed at the facility. Once this is done, an estimate of overall system performance is made. The key to a good VA is accurately estimating component performance. When using a quantitative approach, this is done by starting with a tested performance value for a particular PPS component, such as a sensor, and degrading its performance based on how the device is installed, maintained, tested, and integrated into the overall PPS. For qualitative analysis, performance of each component is degraded based on the same conditions, but the performance of the device is assigned a level of effectiveness, such as high, medium, or low, rather than a number. In addition, component performance must be evaluated under all weather conditions and facility states and considering all threats. The following sections introduce the various stages and activities of a VA.

Planning the Vulnerability Assessment

Before a VA can be performed at a facility, a certain amount of preliminary work must be done to plan and manage the VA so that the customer is provided a useful product. The use of common project management principles and techniques provides a structure and a well-accepted method of approaching the technical, administrative, and business aspects of a VA. At a high level, a project can be broken into three major stages: planning, managing the work, and closeout.

Project Management. Projects, by their definition, have a defined start and end date. There is a point in time when the work did not exist (before the project), when it does exist (the project), and when it does not exist again (after the project). Many VA projects start with an initial customer contact, perhaps as a follow-on to existing work, a reference from another person or business, or as a result of a marketing activity. Project planning starts with understanding what the customer wants or needs. This stage of the project normally involves meetings with the customer to discuss what problems they are having or want to avoid, to understand why they are motivated to do this now, and to discover any specific constraints they may have. Defining the project includes determining the scope of work, as well as what needs to be done, over what period of time, and the cost of the final product. The project scope should state the project objectives and major constraints, such as dollars available or time to complete. Generally, the project is defined in a master document, statement of work, contract, memorandum of agreement, or some other equivalent document. This master document is usually supplemented by a requirements document, which is a summary of the technical specifications or performance required for the delivered product.

After the project has been approved, the customer has sent funding, the project team has been identified, and other administrative issues are set, the actual work can begin. Managing the project includes providing customer support; following the project plan; resolving major and minor project issues on a timely basis; and keeping the project on schedule, within budget and scope, and performing as expected. All of these aspects of the project are organized so that communication between the project leader and the customer and the project team occurs regularly, project risks are managed, product quality maintains an acceptable level, and all project metrics are monitored and remain in compliance.

At some point, all the direct project work is completed, all deliverables are in the customer's hands, the last status reports to the customer have been provided, and the project is complete; however, there are still some remaining issues that must be addressed before pronouncing the project complete. Project closeout can be broken into three areas: financial, administrative, and technical. Financial closeout of the project provides a final accounting of all project costs and allocation of funds to complete the project. Administrative closeout tasks include collecting all project documentation, storing it in an archive, destroying drafts or working papers that are no longer needed, returning any customer-owned equipment or documents, and verifying that all sensitive information is properly marked

and stored securely. The technical closeout of the project can include a project closeout meeting, a lessons learned review, and a closeout report to the customer or internal management.

The use of good project management principles, tools, and skills will help scope, define, manage, and complete a successful VA project for both the VA provider and the customer. A combination of project planning and management techniques minimizes the effects of inevitable project problems and provides a framework to work through major project hurdles.

Establish the Vulnerability Assessment Team. The functional responsibilities of a VA team require a project leader and appropriate subject matter experts (SMEs). Many VA teams will use only a few personnel to serve these roles. Each team member may perform multiple functions, but all appropriate functions must be performed for a thorough VA. The major roles and responsibilities of the VA team include:

- Project Lead
- Systems Engineer
- Security System Engineer
- SME—Sensors
- SME—Alarm Assessment
- SME—Alarm Communication and Display (AC&D)
- SME—Entry Control
- SME—Delay
- SME—Response
- SME—Communication Systems
- SME—Analyst
- SME—On-site Personnel

All members of the VA team should understand their roles and responsibilities, including what information or activities they are expected to contribute to the overall assessment.

Project Kick-off Meetings. Before starting the VA, it is helpful to have kick-off meetings with the project team and the customer. The project team kick-off meeting is meant to familiarize all team members with the project scope, deliverables, schedule and funding and to answer any questions. The project leader should provide the team with a detailed description of the project including the customer's objectives, the project schedule and budget, a review of any travel arrangements that must be made, the deliverables and their format, and how customer contact will be managed. This meeting is also the time to start planning the VA. An overview of the facility layout, geography, weather, and operations can be presented, along with any information concerning threats and targets. Usually, the tools that will be used in the analysis are known, but if not, this is a good time to initiate discussion about appropriate analysis tools.

It can be useful to summarize all of the known information about the project and facility in a VA team guide. This guide serves as a means of communicating information to all project team members and as a living document that captures facility information. The guide is a reasonably detailed description of the planned activities, but does not need to be extremely lengthy. It is expected that some portions of the guide will be common to all VAs and some portions will be unique to a specific facility. The team guide should include the background of the VA, how it will be conducted, team assignments, logistics, and administrative details.

Whatever the scope of the VA, a variety of site-specific data is required to complete the planning phase of the VA. This information is necessary to plan and carry out the VA in the most efficient and least intrusive manner possible. The more this information is known before the team gets to the facility, the easier and faster the VA will be, thus limiting the cost and duration of the team visit. Typical information required includes drawings of the facility, number of employees, operational hours, locations of critical assets, existing PPS equipment, weather conditions, on-site personnel contact information, and location of a workspace for the VA team. If known, this information is included in the team guide.

Another important aspect of the VA project is a briefing to senior management of the facility that will be evaluated. The better the purpose of the VA is communicated to management, the easier the evaluation will be, with few objections to team activities. This briefing should be clear

about the goals and objectives of the VA, how it will be used, when it will be completed, and how the results will be communicated. For some facilities, senior management will receive the report directly. For others, the report may be submitted to another group, who will then distribute the results to the facility. Once the VA team arrives on site, it may be necessary to have a kick-off meeting to explain the VA to lower level facility personnel. Senior management, facility points of contact, the facility security manager, operations and safety representatives, the entire VA team, and other stakeholders should be invited to this briefing. If facility management has already heard a briefing on the project, they may not attend, although it is probably good practice to invite them or a representative. It is always a welcome touch to invite the most senior manager at the facility to address the group and express her support of the process; at the very least, the security manager of the facility should be an active part of this briefing, especially if the VA team is from off-site. Every effort should be made to provide a kick-off meeting at the start of the VA, but if this is not possible, the project leader should be prepared to brief managers and staff at the facility before collecting data in each of the functional areas.

Protection Objectives

To successfully complete a good VA, it is critical that protection system objectives are well understood. These objectives include threat definition, target identification, and facility characterization. Each enterprise defines vulnerability assessment and risk assessment differently, and as a result some facilities may not have defined threats or identified assets. At facilities where the threat and assets have not already been defined, this task must be included as part of the VA project, although this is generally part of a risk assessment. This will likely add cost and time to the project; therefore, it is critical to understand this before finalizing these details in the project plan.

Knowing the threat is one of the required inputs to a VA, because the threat establishes the performance that is required from the PPS. We would not evaluate a PPS protecting an asset from vandals the same way we would for a system protecting an asset from terrorists. By describing the threat, the assumptions that were made to perform the assessment are documented and linked to the decisions that are made regarding the need for upgrades. As such, threat definition is a tool that helps facility managers understand how adversary capabilities impact asset protection and helps PPS designers understand the requirements of the final PPS.

In addition to threat definition, the VA team must also have an understanding of the assets to be protected at the facility. As with threat definition, some customers do not have their assets identified and prioritized before performing a VA. In this case, this must be accomplished before performing the VA. There are three methods for target identification including manual listing of targets, logic diagrams to identify vital areas for sabotage attacks, and use of consequence analysis to screen and prioritize targets. After threats have been defined and assets have been prioritized, a considerable amount of information will exist that is used to establish protection system objectives. The volume of information can be combined into a matrix that relates probability of attack, threat level and tactic, and consequence of loss of assets.

Facility Characterization. The major part of a VA is facility characterization, which consists of evaluating the PPS at the facility. The goal of a VA is to identify PPS components in the functional areas of detection, delay, and response and gather sufficient data to estimate their performance against specific threats. The PPS is characterized at the component and system level, and vulnerabilities to defeat by the threat are documented. Data collection is the core of PPS characterization; accurate data are the basis for conducting a true analysis of the ability of the PPS to meet its defined objectives. Accuracy, however, is only one of several factors to consider. The data gathered must be appropriate to the purpose and scope of the VA, and the quantity and form of the data must be sufficient based

on available resources and desired confidence in the results.

A facility tour is usually conducted early in a VA. During the initial facility tour, the VA team begins to gather information regarding the general layout of the facility, the locations of key assets, information about facility operations and production capabilities, and locations and types of PPS components. Review of key documents and selected records are two important PPS characterization activities. These are useful in the evaluation of the effectiveness of a PPS and may begin during the planning phase of a VA. This step of a VA will also include interviews with key facility personnel. Interviews are critical to clarify information and to gain greater insight into specific facility operating procedures. Interviews with personnel at all organizational levels are recommended. Testing is the most valuable data-collection method for evaluating the effectiveness of a PPS. Evaluation testing can determine whether personnel have the skills and abilities to perform their duties, whether procedures work, and whether equipment is functional and appropriate. Evaluation tests include functional, operability, and performance tests. Functional tests verify that a device is on, and that it is performing as expected (i.e., a sensor still has a probability of detection of 0.9). Operability tests verify that a device is on and working (i.e., a sensor is on and detects, but has moved due to vibration so it is aimed at the wrong location). Performance testing is the characterization of a device by repeating the same test enough times to establish a measure of device capability against different threats. (A sensor is tested many times using crawling, walking, and running modes and under day, night, and varying weather conditions to fully characterize the probability of detection and nuisance alarm rate.) Because performance tests are fairly rigorous and require many repetitions over a period of time, they are generally impractical during a VA. Performance testing is typically performed in a laboratory or nonoperational facility.

One of the goals of the VA team before any system analysis is to identify the various facility states that can exist at the facility. A VA is used to establish vulnerabilities at a facility at all times of the day and at all times of the year. As such, the team must understand the various facility states, so they can determine if the PPS is more or less vulnerable at these times. If the team does not identify these states and determine system effectiveness during all of these different states, the VA will be incomplete and may lead to a false sense of protection. Examples of facility states include normal operating hours, nonoperational hours, a strike at the facility, emergencies such as fire or bomb threats, and shift changes. Once all project planning is complete and protection objectives are understood, the VA team is ready to visit the facility and start collecting data.

Data Collection—Detection

The detection function in a PPS includes exterior and interior intrusion sensors, alarm assessment, entry control, and the alarm communication and display subsystem all working together. Intrusion detection is defined as knowledge of a person or vehicle attempting to gain unauthorized entry into a protected area by someone who can authorize or initiate an appropriate response. An effective PPS must first detect an intrusion, generate an alarm, and then transmit that alarm to a location for assessment and appropriate response. The most reliable method of detecting an adversary intrusion is through the use of sensors, but this can also be accomplished by personnel working in the area or the on-site guard force. Exterior sensors are those used in an outdoor environment, and interior sensors are those used inside buildings.

Intrusion Sensors. Intrusion sensor performance is described by three fundamental characteristics: probability of detection (P_D), nuisance alarm rate (NAR), and vulnerability to defeat. These three fundamental characteristics are heavily dependent on the principle of operation of a sensor and the capability of the defined threat. An understanding of these characteristics and the principle of operation of a sensor is essential for evaluating the intrusion sensor subsystem at a facility. Different types and models of sensors have different

vulnerabilities to defeat. Sensors can be defeated by spoofing or bypass, and consideration of these attack modes are part of the VA. Exterior sensors are grouped into three application types: free-standing, buried line, or fence associated sensors. Interior sensors are grouped as boundary penetration, interior motion, and proximity sensors.

Exterior perimeters are generally found only in high-security applications such as prisons, military bases, research facilities, critical infrastructure facilities, and industrial hazardous facilities (i.e., chemical plants). With a large percentage of the critical infrastructure in the United States owned and operated by the private sector, there is more interest in using exterior sensors in private industry since 9/11. If exterior sensors are not in use at a facility, this is an implicit indication that assets are low value or that the expected threat is low and no evaluation is necessary. The overall evaluation of exterior sensors will include attention to details such as sensor application, installation, testing, maintenance, nuisance alarm rate, and performance against the expected threats. If the threat is able to cut, climb, or bridge fences, this must be considered during the VA. The goal of exterior sensor evaluation is to provide an estimate of sensor performance (P_D) against defined threats, along with supporting notes, pictures, and observations that support this estimate. This will help establish the baseline performance of the overall PPS and, if not acceptable, will provide opportunities for upgrade improvements. Factors that will cause performance degradation include nuisance alarm rate and ease of defeat of the sensor through bypass or spoofing.

Interior sensors are used to aid detection of intrusions inside buildings or other structures. Unlike exterior sensors, interior sensors are commonly used at all types of commercial, private, and government facilities. Just as with exterior sensors, there are several factors that contribute to overall sensor performance. The most common interior sensors are balanced magnetic switches, glass-break sensors, passive infrared sensors (PIR), interior monostatic microwave sensors, video motion detectors, and combinations of sensors, usually PIR and microwave sensors, in dual technology devices.

Interior boundary penetration sensors should detect someone penetrating the enclosure or shell through existing openings (doors, windows, and ventilation ducts) or by destroying walls, ceilings, and floors. Early detection gives more time for the response team to arrive; detection should occur during entry rather than afterward. Volumetric detection uses sensors to detect an intruder moving through interior space toward a target. The detection volume is usually an enclosed area, such as a room or hallway. Most interior volumes provide little delay other than the time required to move from the boundary to the target. Common sensors used for volumetric sensing are microwave and passive infrared radiation. Point sensors, also known as proximity sensors, are placed on or around the target to be protected. In a high-security application, point sensors usually form the final layer of protection, after boundary penetration sensors and volumetric sensors. Capacitance proximity, pressure, and strain sensors are commonly used for point protection, but a number of sensors previously discussed as boundary penetration and volumetric sensors are readily applicable to point protection.

Use of technology is not the only means of sensing intrusions into a facility or area. Employees working in the area, guards on patrol, or video surveillance are other commonly used techniques. These may be effective against very low threats, but testing has shown that these methods will not be effective against more capable threats or when protecting critical assets. Humans do not make good detectors, especially over a long period of time. The lack of firm criteria for what is an adversary intrusion, and the difficulty in recognizing this in time to prevent the attack, as well as safety concerns for employees, all contribute to this problem. Reliable intrusion sensing is best achieved through the use of sensors and is also less expensive than hiring guards. Another weakness of human sensing of intrusions is that it is easier to divert attention away from intrusions, particularly if they are engaged in other activities, such as doing their primary

job, answering phones, or assisting visitors. If the defined threat or asset value is significant, sensing through human observation should be degraded during the VA.

When evaluating interior sensors, the goal is to make a determination of how well installed devices will perform against the expected threat. If sensors are present, there is an implicit expectation that they will be effective in protecting assets. Consideration must be given to the principle of operation of the sensor and its operating environment, installation and interconnection of equipment, NAR, maintenance, and the defined threat. The environment associated with interior areas is normally controlled and is, therefore, predictable and measurable. Consequently, it is possible to evaluate sensors for their performance in a particular environment.

After tours, interviews, and testing are complete, the VA team should document intrusion sensing subsystem strengths and weaknesses. Remember that intrusion detection is just one part of the VA, and the analysis cannot be completed until similar information is collected about the other protection subsystems. This part of the VA concentrates on the probability of detection (P_D) for each sensing type—exterior or interior sensors or sensing by humans. Estimates may be made using qualitative or quantitative criteria.

Alarm Assessment. After an alarm is generated using sensors or human observation, the alarm must be assessed to determine the cause and decide what, if any, response is needed. The detection function is not complete without alarm assessment. There are two purposes of assessment. The first is to determine the cause of each alarm, which includes deciding whether the alarm is due to an adversary attack or a nuisance alarm. The second purpose of assessment is to provide additional information about an intrusion that can be provided to responders. This information includes specific details such as who, what, where, and how many. The best assessment systems use video cameras to automatically capture images that show the cause of an alarm and then display these images to an operator who can assess the alarm. Assessment may also be accomplished through human observation, but this is much slower and not as effective.

It is important to differentiate video assessment from video surveillance when conducting a VA. Alarm assessment refers to direct observation of alarm sources by humans or to immediate image capture of a sensor detection zone at the time of an intrusion alarm. This assessment zone and the captured image can be reviewed to determine the cause of the alarm and initiate the proper response to the alarm. Video surveillance uses cameras to continually monitor all activity in an area, without benefit of an intrusion sensor to direct operator attention to a specific event or area. Many surveillance systems do not use human operators, but record activity on storage media for later review. The most effective security systems will use video assessment and not surveillance to determine causes of alarms.

A video assessment subsystem allows security personnel to rapidly determine whether an intrusion has taken place at a remote location. Major subsystem components include:

- Digital camera and lens
- Lighting system
- Transmission system
- Video recorder and/or storage
- Video monitor
- Video controller

At the end of this part of the VA, an estimate of the probability of assessment (P_{As}) must be provided for use in the system analysis. This probability is a result of the combined effects of video image quality and resolution, speed of capture of images, proper installation and maintenance of all components, and integration of sensor detection zones with camera field-of-view coverage. The most important factor in assessment subsystem evaluation is to verify that video images containing the alarm source provide enough detail to an operator to allow an accurate determination of the cause of the alarm.

Entry Control. The entry control subsystem includes all the technologies, procedures, databases, and personnel that are used to monitor movement of people and materials into and out

of a facility. An entry control system functions in a total PPS by allowing the movement of authorized personnel and material through normal access routes and by detecting and delaying unauthorized movement of personnel and material. Entry control elements may be found at a facility boundary or perimeter, such as personnel and vehicle portals; at building entry points; or at doors into rooms or other special areas within a building. In addition to checks for authorized personnel, certain prohibited items or other materials may also be of interest on entry or exit. For evaluation purposes, entry control is defined as the physical equipment used to control the movement of people or material into an area. Access control refers to the process of managing databases or other records; determining the parameters of authorized entry, such as whom or what will be granted access; when they may enter; and where access will occur. Access controls are an important part of the entry control subsystem.

The primary objective of controlling entry to facilities or areas is to ensure that only authorized persons are allowed to enter and to log these events for documentation purposes. The objective of searching vehicles, personnel, and packages before entry into these areas is to prevent the introduction of contraband materials that could be used to commit sabotage or to aid in the theft of valuable assets. The primary objective of exit control is to conduct searches of personnel, vehicles, and packages to ensure that assets are not removed without proper authorization. A secondary objective of entry and exit control is to provide a means of accounting for personnel during and after an emergency. There are several methods an adversary may use to defeat an entry control point. These include bypass, physical attack, deceit, and technical attacks. Any or all of these methods may be used by the defined threat, and consideration of this is an important prerequisite to entry control subsystem evaluation.

Under operational loads, the entry control subsystem's performance should not adversely impact security or user operations. The system can be divided into two areas with regard to performance—online and off-line functions. Online functions should be treated as a higher priority by the system. These include alarm annunciation, portal access requests, and alarm assessment that require an immediate response to the user. Off-line functions include generation of preformatted alarm history reports or ad hoc database queries.

In addition to the system software, the access control software that commands the entry control subsystem hardware and maintains and manages the data and logic necessary for system operation must be evaluated as part of the VA. In general, the software must receive electronic information from the installed entry control devices, compare this information to data stored in a database, and generate unlock signals to the portal locking device when the data comparison results in a match. Failure to achieve a successful data match will result in a signal that will not unlock the portal.

Many individual entry control technologies are available, as well as many combinations of them that are used in a PPS. In general, these devices are used to control personnel, contraband material, and vehicle entry or exit and include manual, machine-aided manual, and automated operation. The entry control subsystem uses probability of detection as the primary measure of effectiveness. In the security industry the terms false accept rate and false reject rate are also used to characterize entry control device performance. The false accept rate is the complement of the probability of detection and is equal to $1–P_D$. This is a key measurement of subsystem performance, because it represents the probability of defeat of the device. The entry control subsystem can be broken into two major categories: personnel and vehicle control. Contraband material control, such as metal or explosives detection, is a subset of each of these categories.

Alarm Communication and Display. AC&D is the PPS subsystem that transports alarm and video information to a central location and presents the information to a human operator. The two critical elements of an AC&D subsystem are the speed of data transmission to specified locations and the meaningful presentation of that data. Most AC&D subsystems integrate

the functions of detection (detect and assess a potential intrusion) and response (initiate either immediate or delayed response procedures), as well as other subsystems such as radio communications and entry control. Although an AC&D subsystem is a complex integration of people, procedures, and equipment, evaluation by the VA team can be reduced to a handful of performance indicators. Effective AC&D subsystems are robust, reliable, redundant, fast, secure, and easy to use.

The AC&D communications system moves data from collection points (sensor and tamper alarms, video, self-test signals) to a central repository (database, server) and then to a control room and display. If the central repository is physically located in the control room, it may consist of multiple computers or displays, and the communication system may also move data throughout the repository and control room. Alarm communication has several characteristics that compel the evaluation. These characteristics include the amount of alarm data, speed of delivery, and high system reliability.

The control and display interfaces of the AC&D subsystem present information to an operator and enable the operator to enter commands affecting the operation of the AC&D subsystem and its components. The ultimate goal of this subsystem is to promote the rapid evaluation of alarms. An effective control and display system presents information to an operator rapidly and in a straightforward manner. The subsystem also responds quickly to operator commands. The control and display system must be evaluated with the human operator in mind; therefore, operation under conditions not directly related to the AC&D subsystem must be observed during evaluations. The console design should facilitate the exchange of information between the system and the operator, such as alarm reports, status indications, and commands. A good human interface improves the mechanics of issuing commands and of deciphering the information presented. Thus, the amount of data displayed should be limited to only what is required by the operator.

The overriding evaluation principle for the AC&D subsystem must be operator first, and the operator must always be in command of the system. The primary purpose of any AC&D subsystem is to enhance facility security. This is accomplished by making operators more efficient and effective in their duties, thus providing the best protection for the cost of subsystem implementation. An easy-to-use system is much more likely to succeed than an unnecessarily complex one.

The primary performance measure for an AC&D subsystem is the probability of assessed detection (P_{AD}). It is a basic principle of an effective PPS that detection is not complete until an alarm has been assessed, which is why P_{AD} is used as the performance measure for the AC&D subsystem. Factors that contribute to this include time for alarm receipt, time to assess the alarm, ease of system use and control by the operator, and operator workload. This term is the product of probability of detection of the sensor subsystem and the probability of alarm assessment. This formula can be used qualitatively or quantitatively—the key is to verify that both sensors and assessment work together to protect assets. The VA team establishes performance of the intrusion sensing and alarm assessment subsystems individually and then evaluates the AC&D subsystem to show how all subsystems work as an integrated system. P_{AD} is then degraded further based on the results of the evaluation of individual AC&D components. These include:

- Operator workload
- Displays (input/output and ergonomics)
- Video system integration
- Maintenance
- Communications systems for moving sensor data to a display
- Processing systems (computers)
- Other functions (such as entry control)
- Physical infrastructure (power, environmental, cabling, etc.)
- System administration

Poorly integrated AC&D subsystems impact overall system effectiveness by causing decreases in performance in each of the individual components.

Data Collection—Delay

The second function of an effective PPS is delay, which slows down the adversary and allows time for the desired assessment and response. This delay is effective only if it follows detection, which can take different forms. The most obvious form of detection is through the use of electronic sensor systems, which relay information back to a monitoring station. When dealing with truly massive delay barriers such as 15 feet of heavily reinforced concrete or underground bunkers, it may be perfectly acceptable to use humans as the one and only sensor system. Security patrols conducting scheduled or random inspections will be capable of detecting any manual entry attempt with sufficient time to neutralize the adversaries. Increases in adversary task time are accomplished by introducing impediments along all possible adversary paths to provide sufficient delay for any suitable response. In general, estimates of delay times are made using literature searches, actual testing, or approximations made using data from literature or tests. The delay time of any barrier depends on adversary tools and the barrier material. Adversaries have the option of using tactics of force, stealth, deceit, or combinations of these tactics during an attack. Delay evaluation during a VA is primarily directed toward adversary tactics of force or stealth; the entry control subsystem addresses deceit.

To aid alarm assessment and interruption of the adversary at predictable locations, consideration must be given to installing barriers and detection systems adjacent to each other so that the barrier is encountered immediately after the sensor. This delays the adversary at the point of an alarm, increases the probability of accurate assessment, and allows for an effective response. Barrier effectiveness is supported through the use of the principle of balance, which ensures that each aspect of a specific barrier configuration is of equal strength.

A barrier is normally considered as penetrated when an adversary reaches a point 3 feet beyond the barrier. In contrast, defeat is a much broader term, which implies that the barrier is no longer effective in delaying the adversary. This distinction is important because it is quite often easier to defeat a barrier via stealth or other means than it is to penetrate it. Most security barriers at industrial facilities are designed to deter or defeat sporadic acts of vandalism, inadvertent entry, or casual thievery. For more motivated or capable threats, however, these traditional fences, buildings, doors, and locks may present little deterrence or delay.

A close examination of the large variety of scenarios and tools an adversary can select to penetrate a given facility will likely indicate that existing barriers do not ensure that adversary delay time will always be sufficient for the system. Further, if the adversary has not been detected before encountering a particular barrier, or during penetration, the effectiveness of that barrier will be negligible. Most conventional barriers such as distance, fences, locks, doors, and windows provide short penetration delay against forcible (and perhaps stealthy) attack methods that use readily available hand or power tools. Against thick, reinforced concrete walls and other equally impressive-looking barriers, explosives become an effective, rapid, and more likely method of penetration by a determined adversary. An example is the use of vehicle bombs. In addition, recall that security guards are not an effective delay unless they are located in protected positions and are equipped as well as the adversary (i.e., armed adversary and unarmed guards).

An important concept in delay evaluation is that delay is a strong function of the defined threat and adversaries' skill. Stealth, cunning, and surprise can be valuable assets to any adversaries. The VA team should not only look at the physical delay elements present in a PPS, but also look at their condition and integration with the rest of the PPS. The team must consider unique ways that an adversary team could and most likely would exploit weaknesses in the PPS. One of the often overlooked aspects of a VA is how the adversary can, and will, use existing tools and materials within the facility to achieve their goals.

There are a variety of active or passive barriers that can be used to provide delay, and many are present in the normal course of building construction. Depending on adversary tools and capabilities, these barriers will have different delay times. Location of the barrier also plays an important role in the delay time and effectiveness of a barrier. A thick concrete wall on the exterior of a building may be susceptible to rapid breaching with explosives. The same wall, however, when incorporated into an interior underground vault may provide substantial delay, as the adversaries may not be able to use large quantities of explosives without collapsing the entire structure around them. Typical barriers include fences, gates, turnstiles, vehicle barriers, walls, floors, roofs, doors, windows, grilles, utility ports, and other barriers.

Data Collection—Response

Response is the third and final function of a PPS that is evaluated during a VA. There are many ways to respond to a security event; the appropriate response depends on the defined threat, the value of the asset, and the use of risk management options other than a physical protection system at the facility. At any given facility, one or more response strategies may be in use, and this will affect data collection activities accordingly. In addition to the response strategy, security communication is a critical part of any response function and must also be considered during the VA.

The key information collected during the VA relates to two important and interrelated factors. The first is the time it takes for the desired response to be placed into effect; the second is the effectiveness of that response. These aspects of response are facilitated by reliable communication among the responders and with others. A related matter is whether there is an immediate on- or off-site response. During the initial design and implementation of a PPS, each facility must decide if the response goal is to react after a successful attack or to stop the adversary from completing a successful attack. The misalignment of response goals and protection objectives at a facility will cause serious degradation of PPS effectiveness.

Response goals can be broadly categorized as delayed or immediate, respectively. Delayed response refers to any after-the-event reaction, where preventing a successful attack is less important than initiating asset recovery or investigation procedures, or where evacuation of the facility is the response to an attack. Examples of delayed response include review of surveillance tapes after an asset has been lost or damaged, incident investigation, asset tracking and recovery, criminal prosecution, or any combination of these. Immediate response refers to the timely deployment of any personnel to an intrusion to prevent undesirable events from occurring or to the immediate implementation of a mitigation procedure, such as evacuation, after a successful attack, to limit the effects of undesirable events. Generally speaking, if there is no immediate response to security events, there is a basic assumption that the asset can be lost and that this risk is acceptable. This may be true when the asset value is low, the threat is not very capable or motivated, the frequency of the event (i.e., the probability of attack) is low, or the asset is protected using another risk management alternative (i.e., insurance) rather than physical protection, or if liability concerns limit the use of an immediate response. For critical assets, however, the lack of an immediate response to a malevolent intrusion increases the risk of asset loss; therefore, it must be carefully considered during the VA.

The two measures of an immediate response are the time for arrival and neutralization. The time to arrive is used to establish interruption; neutralization is a measure of response effectiveness, given arrival. Interruption is a measure of the detection, delay, communication, and response functions of the PPS and is represented by the probability of interruption (P_I). Neutralization measures response force numbers, training, tactics, and use of any weapons or equipment and is represented by the probability of neutralization (P_N). In addition, the VA team must estimate the probability of communication (P_C), which is essential for an effective immediate response.

Several general response strategies can be used at any given facility; some high-security sites with multiple critical assets may use more than one strategy, and the response strategy plays a major role in how a facility is evaluated during a VA. Response strategies include deterrence, denial, containment, and recovery. Deterrence is used to discourage some low-level threats from attacking a facility by presenting the appearance of tight security, suggesting that an attack would not be successful. This strategy is used at almost all private and government facilities. Because this strategy relies on the adversary's perception that they are not likely to succeed, this approach will work only against less capable or motivated threats.

For some critical assets or production facilities, such as hazardous chemical, biological, and nuclear materials or toxic waste, where release of these agents into the environment through sabotage would cause many injuries, deaths, or contamination, a denial strategy is required. Denial refers to the protection of material by preventing adversary access to areas where materials are stored or to vital equipment used to process the material. For a successful sabotage event to occur, the adversary only has to complete the attack on the target and cause the release; capture of the adversary after a successful release does not prevent the consequence of the attack.

A containment strategy is generally used when the adversary goal is theft of an asset. Containment means that the adversary is not allowed to leave the facility with the asset; that is, they are contained on-site and the theft attempt is not successful. This strategy is usually reserved for facilities with high-value or high-consequence assets, such as mints that store large quantities of currency, museums, precious gem or metal repositories, or hazardous material storage locations. Prisons also use a containment strategy, but they are attempting to prevent inmates from leaving a facility, not the theft of assets.

In the event that deterrence or containment strategies fail, a backup approach is recovery of the stolen asset. In some recovery strategies, the recovery is immediate (i.e., hot pursuit of the adversary as he/she speeds away in a car). For most facilities, there is an acceptance that assets may be lost for a period of time, and recovery of the assets at some point in the future is the primary response. Recovery responses include investigation, tracking of assets, and follow-up using criminal prosecution.

Security communications consist of the people, procedures, and technology used to transmit communications among members of the response force during both normal and response operations. During normal operations, security communications may be required for conducting entry control, escort, patrols, and other security functions (for an on-site security group). During response to an attack, communications are essential for organizing responders, directing them to the scene of the emergency, and successfully interrupting or neutralizing the adversary. Accurate and reliable communication is required for interruption and neutralization. The overall performance measure used is the P_C, which is a measure of confidence that information will flow through the system, starting with alarm reporting and ending with deployment and engagement with the adversary. For a delayed response using video surveillance or assessment, P_C will depend on the transmission system used to capture and store alarm and video information for later review.

The actual performance measures and estimates used depend on the response strategy and the presence of an immediate response. For delayed responses, it is sufficient to ensure that there is timely and accurate detection, and that legally admissible and usable video information is captured as evidence. This requires a fully functional communication system, limited in this case to integrated sensing and video assessment, and transmission of this information to a storage location. This can be approximated using the probability of assessed detection. For any immediate response, response force time, neutralization capability, and the probability of communication will be the key aspects of the evaluation.

Analysis

After all the appropriate data have been collected, analysis of the PPS can begin. There are two basic analysis approaches used in a VA: compliance or performance based. Compliance-based approaches depend on conformance to specified policies or regulations; the metric for this analysis is the presence of the specified equipment and procedures. Performance-based approaches actually evaluate how each element of the PPS operates and what it contributes to overall system effectiveness. The use of compliance- or feature-based systems is only effective against low threats, when assets have a low consequence of loss, or when cost-benefit analyses have been performed that document that physical protection measures are not the most cost-effective risk management option. A compliance-based analysis is easier to perform because the measure of system effectiveness is presence of prescribed PPS equipment, procedures, and people. The analysis consists of a review of facility conformance to the compliance requirements, the use of checklists to document presence or absence of components, and a deficiency report that notes where the facility is out of compliance. The VA report summarizes these findings and the facility makes improvements according to enterprise policy. Because the premise of this text is that overall system effectiveness is the goal of a VA, and that all dollars spent on PPS elements should result in improved protection while also complying with requirements, this text primarily addresses performance-based analysis. Performance-based analysis can use either qualitative or quantitative techniques.

When conducting either a qualitative or quantitative performance-based analysis, the following six-step process is used:

1. Create an adversary sequence diagram (ASD) for all asset locations.
2. Conduct a path analysis, which provides P_I.
3. Perform a scenario analysis.
4. Complete a neutralization analysis, if appropriate, which provides P_N.
5. Determine system effectiveness, P_E.
6. Develop and analyze system effectiveness upgrades, if system effectiveness (or risk) is not acceptable.

If desired, a facility may also choose to evaluate the PPS using risk as a metric, although this method is more commonly used in risk assessment and not in vulnerability assessment.

An ASD is a functional representation of the PPS at a facility that is used to describe the specific protection elements that are present. It illustrates the paths that adversaries can follow to accomplish sabotage or theft goals. Because a path analysis determines whether a system has sufficient detection and delay to result in interruption, it is conducted first. The path analysis uses estimated performance measures, based on the defined threat tools and tactics, to predict weaknesses in the PPS along all credible adversary paths into the facility, measured by the probability of interruption. This step is facilitated through the use of an ASD of the facility to be analyzed.

A scenario analysis is conducted to determine whether the system has vulnerabilities that could be exploited by adversaries using varying tactics, resulting in lower effectiveness of the PPS. Scenario analysis considers specific tactics along the path, as well as attacks on the PPS or on the response force. These tactics include stealth, force, and deceit, and they may be used individually or combined during a scenario. As in path analysis, an important aspect of scenario analysis is consideration of different operating states at the facility or near the asset. There are usually at least two facility states—open and closed. As a part of scenario analysis, an effort is made to identify the worst cases of attack scenarios. Although analysis is not limited to these situations, they are very useful because they define the adversary attacks that test the limits of PPS effectiveness.

After weak paths and suitable attack scenarios have been determined, a neutralization analysis can be performed. This part of the analysis is performed only at facilities where there is an

immediate response resulting in a face-to-face confrontation with adversaries. Neutralization analysis provides information about how effective the response function will be under different scenarios and is a measure of response force capability, proficiency, training, and tactics.

At this point PPS effectiveness can be calculated, using qualitative or quantitative techniques. System effectiveness is represented using only P_I (as in the case of a delayed response using review of video and investigation, when the mere presence of an immediate response will chase an adversary away, or when an adversary will surrender if interrupted), or through the use of both P_I and P_N (at facilities where an immediate response will engage with the adversary).

If the baseline analysis of the PPS shows that the system does not meet its protection objectives, the VA team can suggest upgrades that will address these issues. Usually, these upgrades are not specific technical recommendations, but are functional improvements that can be achieved by increasing performance at certain locations. The analysis is then repeated using these performance increases to estimate the overall increase in the ability of the system to meet its objectives. These results are provided to security system designers who will determine which specific equipment or other upgrades will provide the required performance. Once the analysis is completed, it is important to present both the baseline and upgrade analyses to establish the need for improvements and show the return on investment in upgrades.

REPORTING AND USING THE VULNERABILITY ASSESSMENT

After analysis of facility data is complete, the VA team reports the results in a manner that is useful to the managers at the facility. The goal of the report is to provide accurate, unbiased information that clearly defines the current effectiveness of the PPS, along with potential solutions if the current system is not effective. The VA informs facility management of the state of the PPS and supports upgrade decisions. In general, the VA report is then used in successive projects that address the identified vulnerabilities and improve the PPS at the facility.

Reporting can be formal or informal, verbal or written, and may take the form of a short overview, or a longer, more detailed approach. The choice of reporting form and content is an aspect of the project agreement and generally follows the conventions of the customer or facility being evaluated. Regardless of how reporting is presented and documented, certain content must be included to make the report understandable and useful to the facility. By its very nature, a VA report is a powerful document and should not be shared indiscriminately. Protection of the final report, as well as the appropriate distribution, should be defined as part of the master project agreement. It is recommended that one organization has final control of the document and who it is shared with, even though other organizations may have copies.

Once the VA report is completed, a variety of responses or next steps can take place. By far, the most common approach is for the facility to pursue improving the PPS and following the recommendations of the VA team. A VA can be thought of as the analysis of system requirements that must occur before system design and implementation. The same things that made a particular PPS weak can limit the effectiveness of any upgrades if they are not carefully considered. This process may be relatively short and easy if the recommendations involve only procedural or minor equipment changes, such as replacing one type of CCTV camera with another. If the system requires major equipment upgrades, however, the proper approach to the upgrade design will ensure a cost- and performance-effective result.

The goal of the design team is to create upgrades that meet the performance predicted in the upgrade analysis phase of the VA. This can be difficult to accomplish, and it can take several iterations between the designers and the facility to clarify goals and constraints and to create the best system that can be installed for the available funding. The three general stages of design activity include conceptual, preliminary, and

final design. Although this discussion is focused on the VA of an existing facility, the same process is used for evaluation of a new facility. For new facilities, VA analysts and designers work together closely to model the proposed PPS at the facility, and then iterate on which PPS elements will give the most cost-effective solution. Once they agree, the system designers work through the design stages to define how the final design will be implemented to meet the specified performance.

SYSTEMS ENGINEERING AND VULNERABILITY ASSESSMENT

This section introduces the systems engineering process and describes how this process is used in a VA. Before discussing this relationship, a few definitions and a brief introduction to systems engineering are provided.

In the *Design* textbook, a system was defined as "an integrated collection of components or elements designed to achieve an objective according to a plan." Systems may be small (a microwave oven) or large (a city), and all systems are composed of other smaller systems (or subsystems). In some applications, a collection of many systems into a functional whole is called a system of systems or a family of systems. Further, systems are not found only in engineering, but exist in other disciplines as well. For example, there is a criminal justice system that includes law enforcement, the courts, and corrections. Biological systems can be microorganisms, a pond, or a human. A social system includes the culture, behaviors, and mores of a society. Systems engineering

> *…is an interdisciplinary approach and means to enable the realization of successful systems. It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, and then proceeding with design synthesis and system validation while considering the complete problem. Systems engineering considers both the business and the technical needs of customers with the goal of providing a quality product that meets user needs.*

It is concerned with the integration of functional, technical, and operational requirements within the business goals and environment of the customer. Integration refers not only to physical or electrical integration (although these are important aspects of system performance), but also to the integration of customer needs, technical performance, safety, reliability, procedures, personnel, maintenance, training, testing, and life cycle costs of the proposed solution. The systems engineering process flow is shown in Figure 2-4. The process is iterative and should begin at the requirements stage. A VA fits into this stage of the cycle, which guides the other stages. The results of the VA are used to establish the requirements

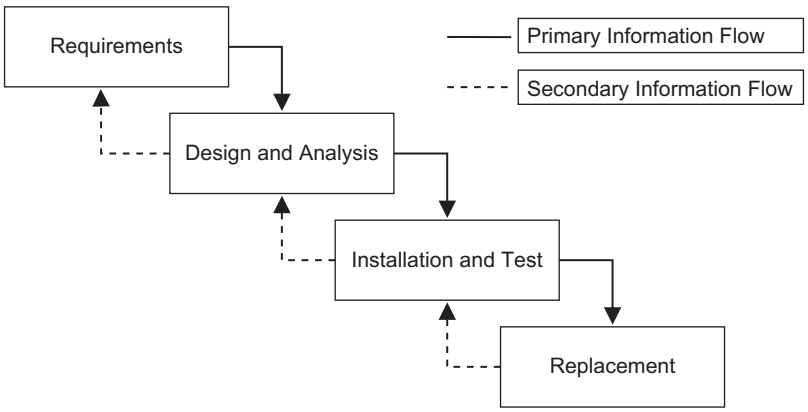


FIGURE 2-4 Systems engineering process.

for an upgraded system design, which are validated through the use of analysis and testing. Once installed, the system should be tested and maintained to optimize system performance and allow for some expansion. At some point, requirements may change or the system reaches the end of its usable lifetime, and replacement of the system or components must be addressed.

Systems engineering is not about being a good engineer—everyone is a systems engineer in his/her area of expertise. Rather, systems engineering is a logical and structured process that starts by defining the problem to be solved, considering multiple potential solutions, and then analyzing these solutions to support selection and implementation of the most balanced and robust design that meets requirements and goals. Implementation of the design includes proper installation, maintenance, testing, and training of personnel to preserve optimal system function. Systems engineering also addresses the final disposition, retirement, or replacement of the system after its useful lifetime has been reached. The information presented in this section is an overview of systems engineering based on principles developed by the International Council on Systems Engineering (INCOSE) and a text by Martin. An effective VA follows basic systems engineering principles.

A common model of systems development is one that considers both systems and component engineering. These two areas are both science based, where science determines what is, component engineering determines what can be, and systems engineering determines what should be. The systems engineering domain includes user requirements (define the problem) and system requirements (boundaries and constraints), which lead to the component engineering domain. This domain includes component selection, design, analysis, integration, and testing.

During a VA, the project leader generally serves as the systems engineer who ensures that the final product meets customer needs, although large projects may include a systems engineer as a separate team member. Component engineers are the subject matter experts on the VA team who bring technical depth in engineering, adversary and response tactics, explosives, analysis, and other areas to evaluation activities.

Because the VA process described in this chapter is performance based, it embraces all the areas of system development described previously: science, systems, and component engineering. The science-based nature of this approach cannot be ignored. An example may clarify the distinction between compliance- and performance-based approaches. A compliance-based approach might select a radar to provide exterior intrusion detection instead of other sensors, such as microwave, active infrared, fence-associated, or buried cable, based on past use, a large inventory of available devices, approved lists, or vendor-provided information. In contrast, a performance-based approach would begin by ensuring that all system requirements are identified and that the selected device is the one that best meets all requirements. Then, performance of the device is based solely on the trade-off analysis of which devices meet all requirements. Examples of exterior intrusion detection requirements include probability of detection, nuisance alarm rate, vulnerability to defeat by the defined threat, integration with other PPS components, expansion capability, and life cycle cost of implementation and operation. This example emphasizes the need for good systems engineering, so that the VA and any necessary upgrades provide the best PPS for the cost. As a result, customer desires often must be bound by explaining what realistically can and cannot be achieved using PPS components. This rationale is included in the requirements stage of systems engineering, which is described next and is a part of VA project management. A brief comparison of compliance- and performance-based approaches is shown in Table 2-1.

Given this background, Figure 2-3 illustrates the systems engineering process as applied in a VA, which will be discussed in other chapters. The remaining sections of this chapter describe the phases of systems engineering in more detail and how they relate to a VA, and include references to specific chapters in the book that contain further information. The purpose of this discussion is not to thoroughly describe the systems

TABLE 2-1 Comparison of Compliance- and Performance-based Vulnerability Assessment Approaches*

Criterion	Compliance-based Approach	Performance-based Approach
Asset value	Low	All assets
Requirement basis	Policy	Overall system performance
Component performance measure	Presence	Effectiveness and integration
Data collection methodology	Site survey	Site evaluation testing
Analysis	Checklist	System effectiveness
Reporting	Deficiency report	Path effectiveness and vulnerabilities
Upgrade design	Address deficiencies	Functional performance estimates
Component selection	Component engineering	Systems engineering
Underlying process	Satisfy policy requirement	Systems engineering

*Compliance-based approaches are less rigorous and easier to perform than performance-based approaches. Compliance-based approaches are most appropriate for low-value assets, whereas a performance-based process can be used for assets of any value.

engineering process, but to show how a VA is based on the process.

System Requirements

As shown in Figure 2-3, evaluation of a PPS begins with an understanding of the problem that is to be solved. This includes facility characterization, defining the threat, and target identification. In systems engineering, these PPS objectives are a subset of system requirements, and they serve as the primary basis for appropriate PPS evaluation by subject matter experts from a variety of disciplines.

A requirement is a characteristic that identifies the levels needed to achieve specific objectives under a given set of conditions and is a binding statement in a contract or regulatory document. In formal systems engineering documents, requirements can be thresholds or goals; thresholds are something that must be achieved, whereas goals have some degree of usefulness or desirability, but are not necessarily mandatory. Requirements are generally stated as "shall," whereas goals are stated as "should." This is a major point to consider when establishing system requirements. There are many customer, user, and stakeholder wants, needs, and expectations. Early in the evaluation process, these imprecise statements must be reduced to an actionable and measurable set of mandatory requirements, so that the final product delivers what the customer expects. It is not uncommon to skip this step in the process and jump immediately into system evaluation. This approach almost always leads to dissatisfied customers and incomplete products and should be avoided. There are three types of requirements in a system: functional, constraint, and performance.

A functional requirement describes the product and level of detail, including component interfaces and what the PPS will do. These requirements address the integration of people, procedures, and equipment that provide the desired end product. They also address stakeholder, customer, and user needs, desires, and expectations. There is a difference in the needs of stakeholders (those who have a role in or expectations of the product), customers (those who pay for the system), and users (those who will operate and maintain the final product). A requirements analysis considers these different needs. These questions are appropriate for customers and stakeholders: What needs are we trying to meet? What is wrong with the current system? Is the need clearly articulated? Other questions concerning who the intended users are, how they will use the product, and how this is different from the present operation are appropriate for users.

Constraint requirements include any external or internal compliance condition or stipulation

that must be met. They include external laws and regulations, legal liabilities, standards, and enterprise policies and procedures. Examples are federal safety requirements, labor law, fire and electrical codes, enterprise-defined infrastructure, and project management processes. In a VA, additional constraints are a function of the specific site, such as terrain, weather, facility layout and footprint, the presence of a response force, and other unique conditions. These constraints are part of the operational environment that must be considered in the VA. Other constraints may be imposed by the limits of available technology, such as the previous radar example.

Performance requirements define how well a capability must operate and under what conditions. These are stated in clear, unambiguous, and measurable terms. Examples of performance measures are earned value, monthly financial status, milestones met, other business or administrative measures, and security performance measures such as probability of detection, delay times, probability of assessment, and probability of interruption. Performance requirements are derived from functional requirements and specify the metrics that are used to judge component and system effectiveness in meeting requirements.

There are many reasons to perform a VA, and these underlying needs must be understood by the VA team before beginning the evaluation. For example, periodic VAs may be required by an enterprise policy or regulatory agency (a constraint requirement), even though the system is still performing as required. Or, the facility may have recently been attacked and lost a critical asset, and there is a desire to improve protection of assets (a functional requirement). Since 9/11, many private companies and government agencies have issued new threat guidance concerning the use of weapons of mass destruction and need to perform VAs to verify that existing PPSs are still effective (a performance requirement). These examples emphasize the need to understand customer goals in asking for a VA. In addition, the customer's intended use of the VA must be considered. If the VA is performed only to satisfy a regulatory requirement, but there is no intention of implementing any changes in response to identified vulnerabilities, this is important for the VA team to understand. If the customer is unwilling or unable to allocate additional funding or other resources to improving the PPS if required, this is part of the operating environment that constrains the VA. Identifying customer needs, motivation, and desires is a part of VA project management.

In a VA, functional requirements can be equated to defining the protection objectives—what is to be protected (assets) and from whom (threat). A high-level functional requirement in security is "protect the secret rocket fuel formula from theft by a competitor." In addition to these requirements, it is also important to characterize the enterprise in terms of its mission and the external and enterprise operating environments, particularly with respect to any compliance constraints that must be met. For example, since 9/11 a variety of laws and mandates have been enacted by the U.S. government that have had a significant impact on security at airports and seaports. These new constraint requirements must be considered during VAs at these sites, so that their affect on overall system effectiveness is considered.

The performance requirements of the security system are related to the capability of the defined threat. For example, a PPS that protects assets from vandals requires lower performance than one against a group of highly motivated and well-equipped environmental activists. This is why it is so important to define protection objectives before starting the VA and not jump right into design, or worse, procurement, of PPS components. In many instances, an enterprise has responded to a security incident or regulatory requirement by buying more cameras, with no analysis of what capability the new cameras will add to the current system. This relates to the earlier point concerning thresholds and goals. As applied to a VA, a threshold is used to specify the minimum acceptable performance of the PPS that must be achieved (i.e., probability of detection must be 0.9 for running, walking, and

crawling intruders). If the threshold cannot be met by an improved PPS within the constraints, the system is not implemented or requirements are reduced because analysis does not support making an additional investment in a system or upgrade that cannot meet the minimum functional requirements. Put in different terms, the return on investment (ROI) is zero—additional money was spent with no corresponding increase in the ability of the PPS to protect assets. This is not the traditional interpretation of ROI, where there is a direct financial gain as a result of system improvement. Rather, this ROI is the proactive protection of assets in a structured and reasoned manner. This may pay off indirectly in financial gain by protecting the enterprise's reputation, ensure business continuity in case of an attack, and show external auditors or agencies that reasonable steps were taken to protect high-value assets. If a PPS that meets customer needs and system requirements cannot be implemented, other risk management alternatives should be considered, perhaps in combination. There are often other ways to achieve the customer's goals that are cheaper and more effective than reducing risk using a PPS.

System Design and Analysis

At this point, a clear set of requirements exist and have been agreed to by the customer, and the VA can begin. The system is evaluated by subject matter experts (i.e., component engineers) considering the defined threats and identified assets, and all constraints are factored into the evaluation. A VA on a PPS considers the functions of detection, delay, and response, and evaluates how well people, procedures, and equipment meet all requirements. It is implicit in this approach that the defined threat must physically enter the facility to attack. As a result, standoff attacks from off-site or cyber attacks on networks are not part of the VA of a PPS; these are legitimate security concerns that are addressed in the overall security system for the facility. During a VA, the current system is evaluated based on the system requirements, and analysis is used to show whether the system meets the requirements. If the baseline analysis shows that the system does not meet requirements, potential upgrades are analyzed, but only to a functional level (i.e., specific devices that achieve this performance are not identified). In this case, the VA then establishes a new set of system requirements that is passed to designers for upgrade improvements using the new functional and performance requirements. The upgrade design process is described later in this section.

VA analysis is supported through the use of evaluation tests on installed PPS components, which documents PPS component performance and how this affects the overall system. Any performance deficiencies are documented and used in the analysis. These component deficiencies lead to system weaknesses that can be exploited by adversaries, which is the definition of a vulnerability. For many PPS components, historical test data already exist that are used in analysis. The principles and techniques used to evaluate the detection, delay, and response subsystems and components of the PPS form the core of this text.

The VA analysis process includes the use of trade-off analyses that consider the performance that can be expected for various combinations of PPS elements and assist in selection of performance options that best meet all requirements. A robust design will also look beyond the requirements (i.e., thresholds) and determine how effective the system is in meeting customer desires. For example, analysis of a PPS must show effectiveness against the defined threat; in addition, analyses showing how well the system will perform against higher threats can also be performed to give an indication of system effectiveness beyond requirements. This additional performance documents how effective the PPS will be as threats increase, and if this performance can be obtained for little increased cost, it can be a viable option. This is an example of a customer goal, as compared to a requirement. The analysis shows how an investment in the PPS can be leveraged to add system capability at a low cost, for example, installing larger, high-resolution

CCTV monitors in the alarm monitoring station. It may cost a little more to buy better monitors, but better monitors will make operators faster and more effective at assessing intrusion alarms caused by small objects. As a result, a small additional investment in better monitors will provide more effective alarm assessment capability. This relates to the earlier point about meeting customer goals—implementation of this option should be discussed with and approved by the customer, and consider all impacts to the PPS, such as any increased cost of installation, normal and backup power specifications, and operator viewing distance.

At the end of the VA, analysis either shows that the current PPS is effective in meeting requirements, or it isn't. If not, the VA team will propose various functional and performance upgrades to the PPS that will meet requirements. At this point, the VA is complete, and the final report is written. If the facility chooses to follow the VA recommendations, and assuming that many equipment improvements are needed, another separate group of PPS designers is assigned to design the upgraded PPS. The design of a PPS is a complex subject that could easily fill another book; however, the process is summarized in the remainder of this section.

The design stage of the systems engineering process is often iterative, starting with conceptual design, proceeding to a preliminary design, and ending with the final system design that is deployed. As the design progresses, a multidisciplinary team (much like the team that performed the VA) reviews potential design options to converge on the best solution. In many cases, the existing requirements may not completely specify the performance required of the upgraded system, and this is part of the reason for an iterative design cycle. This process is facilitated by the use of design reviews, modeling and simulation tools, test data, and discussions with the customer to verify that the proposed solution is in alignment with their needs (shall requirements) and desires (should requirements). The final design ends in a detailed description of the product and how it is implemented (a detailed final drawing package). Before implementing the final design, the system components are analyzed to validate and verify system operation. Validation is the process of checking satisfaction of stakeholders (have we done the right job?) and verification checks that the design meets the specified technical requirements and the components are properly integrated (have we done the job right?).

Validation checks to ensure that no requirements were missed and that there are no extraneous requirements. This is called requirements traceability and is frequently used in large, costly systems (and may be required by some customers). Traceability shows that the product is just what the customer wanted, no more and no less. It also serves to document and explain selection of specific components during the system design stages and links requirements to these components and the overall system. If there is no link between a component and a requirement, the customer was given more than they needed. This is important because it clarifies for the customer why one device was used over another in the final design. Consider the example of specifying a camera in a PPS design. Many types of cameras are available, and selection of the appropriate camera depends on the functional, constraint, and performance requirements of the system. If the defined threat includes an adversary crawling across a perimeter at night, camera resolution, lighting, video recording, and storage must be specified to meet this performance requirement. Contrast this with a defined threat that includes a vehicle crashing the perimeter. The larger profile of a vehicle will not require the same camera resolution as a crawling attacker; thus the specific camera that is selected may be different. However, the vehicle will be moving at a faster rate of speed than a crawler, and this constraint will influence what other devices are incorporated into the system design. Validation often uses acceptance tests under local conditions to check that the system meets the needs and expectations of stakeholders. If formal documentation is needed, the use of traceability software, as noted previously, may be warranted (go to www.telelogic.com for an example). The software documents the link

between requirements, system design, implementation, and test.

System Installation and Test

At this stage of the upgrade process, the new design is implemented as described in the drawings and specifications of the final design package. Deviations from these specifications should be approved by knowledgeable experts who understand their effects on component and overall system performance. Some changes may be relatively transparent, but others may seriously affect system performance. For example, changing the distance between or height of light fixtures may change the amount of light that is available in an area. System installation is supplemented by on-site operational, functional, and performance tests to ensure that the system is working as predicted and the customer's needs are met. Operational tests confirm that an installed device is working (i.e., it sends a signal), and functional tests show that the device is working and performing as expected (i.e., a sensor still has the expected P_D). It is also recommended that final acceptance tests are performed before the customer accepts the delivered system. An acceptance test is the final stage of system delivery, and test results are used to either justify or withhold final payments to vendors, depending on whether the system passes or fails the test.

Because the PPS is expected to continue to perform after initial installation, proper maintenance and periodic testing of components and the system are required to maintain optimal system function. These are aspects of the overall system and system design also includes recommendations on the maintenance, testing, and training procedures that should be used to keep the system operating reliably and as expected. These details are aided by complete system documentation, a preliminary training program to acquaint users with the proper ways to maintain the system, and recommended procedures and processes that will ensure continued acceptable system performance. Component installation, maintenance, testing, and staff training procedures are evaluated during the VA and can have a significant effect on overall system performance. Procedural improvements can also be low-cost system upgrades.

System Replacement

It is good systems engineering practice to include planning for the retirement and replacement of the system in the system design, after its expected lifetime has been reached. The final design that is implemented should allow for system expansion and growth, up to a certain point. Typically, this point allows for 50% expansion above the current capability. This advance planning allows for expansion of systems in response to changes without excessive cost or loss of protection. Examples of system expansion include the installation of fiber optic cable bundles with more conductors than currently needed at initial installation. It only costs a little more to buy a fiber bundle with twice as many conductors; installation costs are the same. Alternatively, a conduit with a larger diameter could be used to allow room for additional wiring at a later date. In the same way, adding power drops or junction boxes will allow for rapid expansion of the PPS in the future. It is expected that technology will advance, threats will change, facilities may grow or shrink, or equipment will fail, any of which can create a need for new components that meet existing or new requirements. Although retirement and replacement are not part of a VA, expansion capability of the PPS is one criterion that is considered during a VA.

SUMMARY

This chapter described risk management, vulnerability assessment, and systems engineering and explained how these processes support security system evaluation. Risk management and risk assessment were reviewed. Both qualitative and quantitative techniques to measure system effectiveness in a vulnerability assessment were described, as well as when each technique is appropriate. The use of statistical measures

was discussed to introduce this topic and to show how statistics are used to support system evaluation. The vulnerability assessment process was also introduced by dividing the process into three stages—planning, conducting, and reporting—and using the results. This chapter ended with a brief description of how the evaluation process described in this text follows a systems engineering process to enable the realization of successful systems. This process focuses on defining customer requirements and then evaluating the system while considering the complete problem. Systems engineering integrates disciplines and groups into a team effort, following a structured development process that proceeds from problem definition to evaluation and analysis to implementation of any required system upgrades, while considering both the business and the technical needs of customers with the goal of providing a quality product that meets user needs.

REFERENCES

[1] Garcia ML. The design and evaluation of physical protection systems. Boston: Butterworth-Heinemann; 2001.
[2] Grose VL. Managing risk: Systematic loss prevention for executives. Arlington, VA: Omega Systems Group; 1987.
[3] Kaplan S, Garrick BJ. On the quantitative definition of risk. Risk Analysis 1981;1(1):11–27.
[4] Haimes YY. Risk modeling, assessment, and management. 2nd ed. Hoboken, NJ: Wiley and Sons; 2004.
[5] International Council on Systems Engineering (INCOSE); April 18, 2005. Definition available at http://www.incose.org/practice/whatissystemseng.aspx.
[6] Martin JN. Systems engineering guidebook: A process for developing systems and products. Boca Raton, FL: CRC Press; 1987.

CHAPTER

3

Security Surveys and the Audit

Lawrence J. Fennelly, CPO, CSS, HLC III

A security survey is a critical on-site examination and analysis of a place, which may be an industrial plant, business, home, or public or private institution to ascertain the present security status, identify deficiencies or excesses, determine the protection needed, and make recommendations to improve the overall security. Your survey or audit must include the external and internal complex, as well as the identification of threats, identify controls, level of risk and your completed risk assessment, which should include risk analysis, risk identification, and risk evaluation.

It is interesting to note that a definition of *crime prevention* as outlined by the British Home Office Crime Prevention Program—"the anticipation, recognition and appraisal of a crime risk and the initiation of action to remove or reduce it"—could, in fact, be an excellent description of a security survey. The only difference, of course, is that a survey generally does not become the "action" as such but rather a basis for recommendations for action.

This definition can be divided into five components and analyzed so that its implications can be applied to the development of a working foundation for the security surveyor:

1. **Anticipation.** How does the anticipation of a crime risk become important to the security or crime prevention surveyor? Obviously, a primary objective of a survey is the anticipation or prevention aspects of a given situation—the pre- or before concept. Thus, an individual who keeps anticipation in the proper perspective maintains a proper balance in the total spectrum of security surveying. In other words, the anticipatory stage could be considered a prognosis of further action.
2. **Recognition.** What does an individual need to conduct a survey of the relationships between anticipation and appraisal? Primarily, the ability to recognize and interpret what seems to be a crime risk becomes an important skill a security surveyor acquires and develops.
3. **Appraisal.** The responsibility to develop, suggest, and communicate recommendations is certainly a hallmark of any security survey.
4. **Crime risk.** As defined in this text, a crime risk is the opportunity gained from crime. The total elimination of opportunity is most difficult, if not improbable. Therefore, the cost of protection is measured in (1) protection of depth and (2) delay time. Obviously, the implementation of the recommendation should not exceed the total (original or replacement) cost of the item(s) to be

protected. An exception to this rule would be human life.

5. **The initiation of action to remove or reduce a crime risk.** This section indicates the phase of a survey in which the recipient of the recommendations decides whether to act, based on the suggestions (recommendations) set forth by the surveyor. In some cases, the identification of security risk is made early in a survey and it is advisable to act on the recommendation prior to completing the survey.

The responsibility to initiate action based on recommendations is the sole duty of the recipient of the survey. This is to suggest that the individual who receives the final evaluation and survey is the individual who has commensurate responsibility and authority to act.

Remember a *security risk analysis* is a more in-depth study, including risk management, analysis of risk factors, environmental and physiological security measures, and analysis of crime patterns, fraud, and internal theft. It is a process of assessing threats and risk and the formulation of strategies to minimize the risk and achieve security.

THE BEST TIME TO CONDUCT THE SURVEY

Most crime prevention officers and security directors agree that a survey is most effective after a crisis within the corporation, after a breaking and entering or major larceny, after major changes in physical infrastructure or their operational process, or on request from auditors. There are times when a merchant, hoping to get something for nothing, calls the crime prevention officer in the town to conduct such a survey, when in reality there is no intention of spending a dime for improvement. A security professional conducted a detailed security survey on a factory warehouse and office building. The recipient of the survey followed only one of his recommendations, which was to leave a light on over the safe in the back room of his warehouse. The owner had completely disregarded recommendations such as hardware improvements on doors, windows, and skylights. Unfortunately, thieves returned and almost put him out of business.

WHY CONDUCT A SECURITY REVIEW

There are several reasons to conduct a security review:

1. To identify what needs to be protected.
2. To ascertain current risk/security management needs.
3. To determine the threats and the risk and vulnerability of an organization's assets.
4. To ensure that the security management plan combats identified threats in a cost-effective and proactive manner.

CLASSIFICATION OF SURVEY RECOMMENDATIONS

The various classifications of recommendations can be best explained through an example. The classifications are maximum, medium, and minimum. The example selected is a museum that contains $25 million in various art treasures; the complex has no security.

Maximum Security

Obviously, the museum needs an alarm system; therefore, our maximum security classification recommendation should read:

> *Alarm the perimeter (all exterior and interior doors, all windows and skylights). Four panic alarms to be installed at various locations, and six paintings, which are worth $12 million, should be alarmed—each on a separate 24-hour zone.*

Ultra-maximum security is specifically not mentioned because this term applies to an armed camp—machine guns, guards in full battle dress armed with semiautomatic rifles, grenades, flamethrowers, mines, and locking devices equipped with dynamite, which will blow up when an intruder attempts to pick the lock. It is dramatic

and it is ultra-maximum. It is not ridiculous for Fort Knox to provide ultra-maximum security to protect its billions in gold bullion.

Medium Security

A medium security classification recommendation would read:

> *Alarm all basement windows and all ground floor windows that are at the rear of the building. Install one panic alarm by the main entrance. Alarm the six paintings worth $12 million, each alarm on a separate 24-hour zone.*

Minimum Security

Finally, a minimum security classification recommendation would read:

> *From a risk management point of view, alarm the six paintings worth $12 million, each painting to be alarmed on a separate 24-hour zone.*

First Step

These three examples clearly show the degree of security one can obtain by trying to plan a security package. I stated these examples because your first step in conducting a security survey is an interview with the individual to whom you turn over your report. During this interview, you form an appraisal on the degree of protection required.

Sometimes, you may have to state all three recommendations in a report. Other times, you must be conscious that you may force the receiver of your report to accept less security than you suggest because you did not thoroughly and clearly explain your security points.

DEVELOPING SECURITY POINTS

Like most professionals, we need tools to do an effective job. The following are suggested to assist you when conducting your surveys: tape measure, floor plans, magnifying glass, flashlight, camera with flash, small tape recorder, screwdriver, penknife, pencil, pad of paper, and surveyor's wheel.

Your survey is conducted systematically so that the recipient can follow your recommendations in some kind of order. Start with the perimeter of the building. Once inside the building, start at the basement and work your way to the attic. Do not be afraid to be critical of the area that you are in. This is what the recipient wants. Consider taking photos of the various buildings that are to be inspected; this will aid you with your report and inspection.

After you have done several surveys you will develop a style of putting them together and they become easy. There is software available for security surveys, and these have their place; however, it is not necessary to purchase the software in order to complete the security survey/audit. Also consider a review of ISO 17799, ISO 27001, and ISO 27002 as all three are germane to today's modern security professional.

Dos and Don'ts in Developing a Report

Dos

1. Be honest in your recommendations. You are the expert.
2. Call the shots as you see them. Consider the use of simple language; short sentences are best.
3. Be critical—physically tear the property apart in your mind as part of the process.
4. Keep it as simple as possible, but not simpler.

Don'ts

1. Don't over exaggerate your reports. They are too important.
2. Don't inflate the report with maps and floor plans; however if these plans illustrate vulnerabilities, then they can be very useful. Merely putting them in for filler is a poor practice.
3. Don't repeat your statements.

4. Don't make statements beyond your core capability, certifications, and training. It is acceptable to report allied facts that are germane to the report, but commenting on topics outside of your domain experience is risky, and not a best practice.

The written report should include the following:

Page One: Introduction or sample cover letter.
Page Two:

A. Identification of building, and activities conducted at this property.
B. Specific statement of the major problems in order of priority.
C. Alternative recommendations to the problem and a short list of identified risks and vulnerabilities.
D. List of your further recommendations.

General statements such as the following can be included in the report:

1. Physically inventory all property at least once a year. Your inventory should list the name of the item, manufacturer, model, serial number, value, color, and date purchased.
2. Engrave all property in accordance with the established operation identification program.
3. All computers should be bolted down and all files, cabinets, and rooms containing valuable information or equipment should be locked when not in use.

Other Keys to Being an Effective Surveyor

Only when you have developed the ability to visualize the potential for criminal activity will you become an effective observer. This ability is the part of the process referred to as an art. Nonetheless, it is important that, when you arrive on a survey site, you are prepared to give a property owner sound advice on the type of security precautions to consider. Consider environmental criminology and how crimes occur at specific places, times, and settings, and where offenders, victims, and targets of opportunity coincide. Merely identifying the variables can provide value and greater clarity for the survey.

In summary, to be a good crime prevention practitioner, you have to be a good investigator. You must understand criminal methods of operation and the limitations of standard security devices. In addition, you must be knowledgeable about the type of security hardware necessary to provide various degrees of protection.

NINE POINTS OF SECURITY CONCERN

1. **General purpose of the building (i.e., residence, classroom, office).** Consider the hours of use, people who use the building, people who have access, key control, and the maintenance schedule. Who is responsible for maintenance? Is the building used for public events? If so, what type and how often? Is the building normally opened to the public? Identify the significant factors and make recommendations. Who is the facility manager and who has overall responsibility for crime prevention and security?
2. **Hazards involving the building or its occupants.** List and assign priorities (e.g., theft of office equipment, wallet theft, theft from stockrooms). Identify potential hazards that might exist in the future.
3. **Police or security officer applications.** What can these officers do to improve the response to the building and occupants from a patrol, investigation, or crime prevention standpoint? Would the application of security officers be operationally effective or cost effective?
4. **Physical recommendations.** Inspect doors, windows, lighting, and access points. Recommend physical changes that would make the building more secure, such as pinning hinges on doors and fences.
5. **Locks, equipment to be bolted down, potential application of card control, and key control.** Make specific recommendations.

6. **Alarms.** Would an alarm system be cost effective? Would the use of the building preclude the use of an alarm? Are the potential benefits of an alarm such that the building use should be changed to facilitate it? Consider all types of alarms, building-wide or in specific offices. Consider closed circuit television and portable or temporary alarm devices.
7. **Storage.** Does the building have specific storage problems, such as expensive items that should be given special attention, petty cash, stamps, calculators, or microscopes? Make specific recommendations.
8. **Trespassing.** Are adequate "No Trespassing" signs posted? Are other signs needed such as "No Solicitation" or "No Skateboarding"?
9. **Custodians.** Can custodians be used in a manner that would be better from a security standpoint?

PERSONALITY OF THE COMPLEX

Each complex that you survey has a distinctive personality. Let us take an average building, which is open from 9 a.m. to 5 p.m. The traffic flow is heaviest during this period. During the span from 5 p.m. to 12 a.m., the building is closed to the public. Some staff members may work late. Who secures the building? At 12 a.m., the cleaning crew arrives and prepares the building for another day. The whole personality of the complex must be taken into consideration before your report is completed.

Let us take a further example of building personality. The complex is 100 × 100 feet and it has two solid-core doors, one large window at the front of the building, and is air conditioned.

Case 1. The complex is a credit union on the main street next door to the local police department versus the same credit union on the edge of town.

Case 2. This is a large doctor's office. The doctor is an art buff and has half a million dollars in art in the office versus a doctor who has no art but has a small safe with about $200 worth of Class A narcotics inside.

Case 3. This building houses a variety store that closes at 6 p.m. versus a liquor store that is open until 2 a.m.

In these cases, I give six examples of the personality of a complex. As I stated, your recommendations must be tailored to fit the lifestyle and vulnerabilities of these buildings.

POSITIVE AND NEGATIVE ASPECTS OF MAKING RECOMMENDATIONS

In making your recommendations for security improvements, you must consider the consequences of your suggestion in the event the property owner implements it. Negative as well as positive aspects are involved. Take, for example, a housing complex that has a high crime rate from outsiders and within. Your recommendation is, "Build a 10-foot high fence around the complex."

Positive Aspects

Crime is reduced—the environment can be designed so that the individual considering a criminal act feels that there is a good chance to be seen by someone who will take action and call the police. Another meaningful positive aspect is the fear of crime and if present it also must be addressed.

Vandalism is less—the target of attack can be made to appear so formidable that the person does not feel able to reach the target. It adds to the physical aesthetics of the area through environmental design.

The visual impact is negative—this ensures the property of the residents, adding to their secure environment. Limiting the number of points of entry and establishing access control primarily decreases crime opportunity and keeps out unauthorized persons.

Negative Aspect

A fortress environment may create more of a psychological barrier than a physical one. It is

socially undesirable and yet is replicated throughout our country at an increasing rate.

Community Reaction

This cannot be disregarded. Furthermore, vandalism at the time of early installation should be considered. Get the residents, occupants, employees, etc., involved in the early planning process.

Consciousness of fear may develop by those tenants whose apartments face the fence; but as the tenants come and go, it will eventually be accepted.

All fences are subject to being painted by groups with a cause. Consider using cyclone fencing or other see-through fencing to discourage visible graffiti from being applied to the fence. An eye-pleasing architectural crime prevention through environmental design (CPTED) feature would be to recommend: stones, gardens, terraces, etc., to improve the physical appearance and avoid the stigma of a fortress environment.

CRIME ANALYSIS

It is not necessary for you to be a statistician, but the more you know about and understand the local crime problems, the better equipped you are to analyze the potential crime risk loss in surveying a business or a home.

Crime analysis collection is simply the gathering of raw data concerning reported crimes and known offenders. Generally, such information comes from crime reports, arrest reports, and police contact cards. This is not to say that these are the only sources available for collecting crime data. Police reports, security officers' reports, reports from the fire department, Googling the location on the Internet, and newspapers are all sources available to obtain added data.

The analysis process as applied to criminal activity is a specific step-by-step sequence of five interconnected functions: crime data collection, crime data collation, data analysis, dissemination of analysis reports, and feedback and evaluation of crime data.

Crime analysis of the site you survey supplies you with specific information to enable you to further harden the target in specific areas where losses have occurred. It is a means of responding "after the fact," when a crime has been committed.

KEY CONTROL

Whether a place has physical keys or electronic keys, key control is an extremely important inclusion in a crime prevention or security survey. Check whether the clients are in the habit of picking up physical and electronic keys from employees at their termination and if they have an accurate record of who has which keys. Within a few short minutes, you should realize whether or not the recipient of your survey has a problem.

Almost every company has some sort of master key system, because many people must have access to the building without the inconvenience of carrying two dozen keys around every day. Master keys are required for company executives, middle managers, and the security department, as well as the maintenance department.

Guidelines for Key Control

1. Purchase a large key cabinet to store and control the many keys in your possession.
2. Two sets of key tags should be furnished or obtained with the new key cabinet: One tag should read "file-key, must not be loaned out," and the second tag should read "Duplicate." The key cabinet should be equipped with *loan tags*, which identify the person to whom a key is loaned. This tag is to be hung on the numbered peg corresponding to the key that was used.
3. Establish accurate records and files listing the key codes, the date the key was issued, and who received it. Ensure also that the electronic card keys are used properly and that data is captured and recorded.
4. Have each employee sign a receipt when he or she receives a key.
5. All alarm keys should be marked and coded.

6. A check should be made of what keys are in the possession of guards and staff.
7. Do not issue keys to any employee unless absolutely necessary.
8. Only one person should order and issue keys for the complex.
9. Change the key cylinder when an authorized key holder is discharged for cause. Furthermore, discharged or retired employees should produce keys previously issued at the time of termination.
10. Periodic inspections should be made to ensure that possession of keys conforms to the record of issuance. These periodic inspections should be utilized to remind key holders that they should immediately notify you of any key loss.
11. The original issue of keys and subsequent fabrication and reissuance of keys should ensure that their identity is coded on the keys so the lock for which they were manufactured cannot be identified in plain language.

Electronic key control is also important. Suggest that you have a program in place to delete those badges of termed employees and that it is included in your policy procedures.

DIGITAL CLOSED-CIRCUIT TELEVISION

Digital closed-circuit television (CCTV) is a valuable asset to any security package and an even more valuable tool if hooked up to a digital video recorder (DVR); analog video recorders are still used in some applications, but the merits of DVRs and IP video systems have trumped analog video system components. CCTV is a surveillance tool that provides an added set of eyes. Whether the video system is actively monitored or merely recorded for follow-up depends on the application and requirements for security. If this equipment is on the site you are surveying, it is your job to evaluate its operation and effectiveness:

1. Is it working properly? Is the video quality sufficiently clear to determine the identity of individuals or detect activity in the field of view? Are all of the cameras working? Is the system set up for triggered events (e.g., on motion, door opening, or other dry-contact prompt)? Are the pan-tilt-zoom cameras commissioned for a purpose (e.g., with preset camera view positions at critical areas)? Are privacy zones set up where appropriate?
2. How is it being monitored or recorded, and is the video data being saved for the appropriate number of days? Typically 30 days of storage was the standard for analog video recorder applications; however, 90 days of storage has become the norm for digital video storage, with the capability to save video events on the digital storage permanently as required. You will find that auditors will want 90 days as a minimum to be available.
3. Are the camera fields of views placed where they will be most beneficial?
4. Are the lighting levels in the areas being video monitored sufficient for the setting, place, and activity to be detected?
5. Is the security recording hardware system secured in a locked cabinet or enclosure?

INTRUSION ALARMS

If the site you are surveying already has an alarm system, check it out completely. Physically walk through every motion detector unit. Evaluate the quality of the existing alarm products versus what is available to meet the needs of the client.

I surveyed a warehouse recently that was only 5 years old. It was interesting to note that the warehouse had a two-zone alarm system. The control panel was to the right of the front door, which was about 15 feet from the receptionist. Both alarm keys were in the key cylinders, and according to the president of the company, "The keys have been there since the system was installed." My point is, for a dollar, another key could be duplicated and then the area is vulnerable to attack.

Another time, while doing a survey of an art gallery in New York, the security director stated

that he had not had a service call on his alarm system in 2 years. We then proceeded to physically check every motion detection unit and magnetic contact. You can imagine his reaction when he found out that 12 out of the 18 motion detection units were not working.

In conclusion, intrusion alarms come in all shapes and sizes, using a variety of electronic equipment. It is advisable to be familiar with the state of the art electronics so that you can produce an effective report.

LIGHTING AND SECURITY

What would happen if we shut off all the lights at night? Think about it. Such a foolish act would create an unsafe environment. Senior citizens would never go out and communities would have an immediate outbreak of theft and vandalism. Commercial areas would be burglarized at an uncontrollable rate. Therefore, lighting and security go hand in hand. This example may seem far-fetched, but in fact, installation of improved lighting in a number of cities has resulted in decreased vandalism, decreased street crime, decrease in suspicious persons, decreased commercial burglaries, and, in general, a reduction in crime.

Streetlights

Streetlights have received widespread notoriety for their value in reducing crime. Generally, streetlights are rated by the size of the lamp and the characteristics of the light dispersed. More specifically, four types of lighting units are utilized in street lighting. The most common, and oldest, is the incandescent lamp. It is the most expensive in terms of energy consumed and the number needed. As such, incandescent lighting is generally recognized as the least efficient and economical type of street lighting for use today.

The second type of lighting unit, which has been acclaimed by some police officials as "the best source available," is a high-intensity sodium vapor lamp. This lamp produces more lumens per watt than most other types. It is brighter and cheaper to maintain, and the color rendition is close to that of natural daylight.

The third and fourth types of devices commonly used for street lighting are the mercury vapor and metal halide lamps. Mercury vapor lights have long life but are slow to fully illuminate and are generally dim lighting fixtures with little spread of the illumination beyond the light source. These are typically recommended for single structure locations such as a garage or back alley or access point to an infrequently used walkway. However, when high use of the property is expected, or it is imperative to observe who or what is using a property at a particular place, the lighting source frequently recommended is the metal halide light, which is bright white, with instant on, and provides great white color balance for video recording and human eye observation. This type of light is typically seen at new car lots and gas stations.

Check for lighting standards and lighting levels for particular places one is inspecting: these can be obtained from IES and other standards-making bodies, and from place-specific professional associations (e.g., banking, hospital, health, multi-family housing, etc.).

OTHER SECURITY ASPECTS

Depending on the type of facility you are surveying, the following should be reviewed:

1. Communications networks, utility closets, IP data networks, walkie-talkies or cell phones with walkie-talkie features, and locations of interior and exterior phones
2. Guard force and security personnel and their training, police powers, uniforms, use of badges, and methods of operation (typically called Standard Operating Procedures, SOPs, and Post Orders)

Your objectives are to identify vulnerabilities, evaluate the site, and provide critical assessment. Methodology and style are purely those of the surveyor, but do not forget they also represent a document from you and your department.

SECURITY SURVEY FOLLOW-UP

The follow-up to your security survey takes many forms, from actually sitting down with the recipient to going by the site and seeing if any changes have actually taken place. Some police departments produce five to seven surveys a day. They do not evaluate their performance because of the time and personnel involved. In this way, they fail to examine their own effectiveness. The reason for the follow-up is to encourage increased compliance and ensure that recommendations are understood. Without this step, you will not know if the recipient has taken any action.

The basic security survey framework consists of five steps:

1. Generating the survey request
2. Conducting the physical inspection
3. Delivering survey recommendations
4. Following up after the report is completed
5. Evaluating the program

For every crime committed, there is a crime prevention or loss reduction defense or procedure that, if followed, could delay or prevent a criminal from committing that act.

Physical security involves implementing those measures that could delay or deny the risks, threats, vulnerabilities, and crimes determined during the survey, and these may include but not necessarily be limited to unauthorized entry, larceny, fraud, sabotage, fire, and vandalism. This chapter on security surveys is geared to assist both private security and public law enforcement to harden a target and assist the community to further reduce losses.

To further assist your security survey, several checklists are included at the end of this chapter.

RESIDENTIAL SECURITY

A large percentage of home burglars enter by a door or window. In most cases the front, rear, bulkhead, or garage door is unlocked. Front and rear doors often have inadequate locks or are built in such a way that breaking the glass to the side of the door or on the door itself allows the burglar to simply reach inside and unlock the door. Windows on the first-floor level are the crook's next choice for entry. Basement windows are the least desirable because they may require the burglar to get dirty and, like executives, this person is concerned about appearance. However, a basement is a good location for individuals to hide, thus it becomes much more attractive.

Defensive Measures

1. **Doors (front, rear, basement, and garage).** The first important item is to install dead bolts on all entry doors. A cylinder dead bolt with a 1-inch projecting bolt, made of hardened steel, should be utilized. This lock should be used in conjunction with a standard entry knob lock. Viewing devices with a wide angle lens on entry doors is also standard to prevent unwanted intrusions into the home.
2. **Doors with glass in them.** The back door is one of the burglar's favorite entryways. Most rear doors are made partly of glass, and this is an open invitation to a burglar. This type of door must have a double cylinder dead bolt for protection. This type of lock requires a key to open it from the inside as well as the outside, because most burglars break the glass and try to gain entry by opening the locked door from inside.
3. **Sliding glass doors.** These entries should be secured so they cannot be pried out of their track. Also, you can prevent jimmying of your door by putting a "Charley bar" made from wood or metal and cut to size and placed in the track when the door is closed (Figure 3-1).

Bulkheads should also be included as part of your overall security package and secured with square bolt or dead bolt locks.

Windows

Windows come in a variety of shapes, sizes, and types, each of which presents a different type of security problem. Windows provide an inviting

entryway for a burglar who does not like to break glass because the noise may alert someone. On double-hung sash-type windows, drill a hole through the top corner of the bottom window into the bottom of the top window. Place a solid pin into the hole to prevent the window from being opened (Figure 3-2).

Keyed window latches may also be installed to prevent the window from being opened. In addition, grilles and grates may be installed over extremely vulnerable accesses.

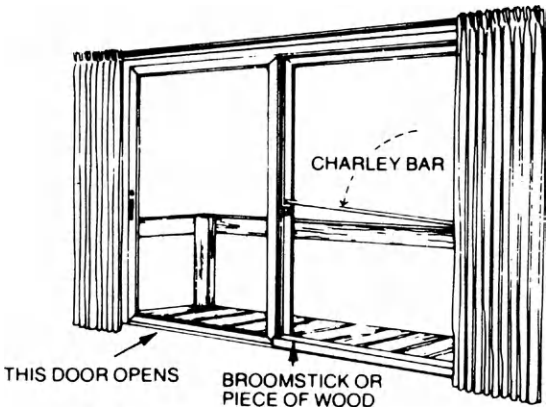


FIGURE 3-1 Preventing force sliding of aluminum doors. Mount a Charley bar that folds down from the side.

Entrances

Any opening through which a human body can pass is an entrance. Front doors, basements, patio doors, garages that have access to the house, and windows on the second floor are all entryways to burglars. No one way is more important to protect than another.

Setting Up Inner Defenses

Even with the precautions already mentioned, a burglar may still get into the home. Once there, you should try to slow down this spree, as time is the one element working against the criminal. One successful method is to convert a closet into a vault, by installing a dead bolt lock on the door. You have now considerably strengthened the inner defenses. Restricting access from one part of the home to another via dead bolts and the like gives the burglar yet another obstacle to overcome.

Having a burglar alarm stand watch is like an insurance policy. The homeowner may never need it, but it is comforting to know it is there. The very best system is a perimeter system that stops an intruder before entering the dwelling,

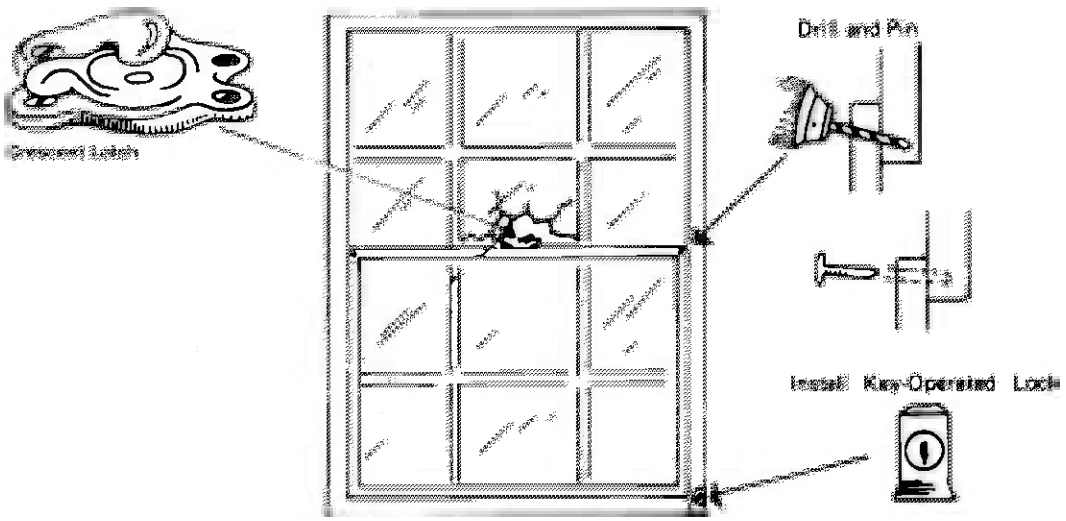


FIGURE 3-2 A double-hung window can be easily jimmied open with a screwdriver. Glass can be broken adjacent to the crescent latch or by prying against hardware, and the screws can be popped out. To prevent this, drill a hole through the top corner of the bottom window and place a solid pin in the hole. You can also install a key-operated lock.

but it is also costly. Less expensive methods involve using pads under rugs and motion detectors.

Remember, no home can be made 100% burglarproof, but in most instances, by making it extremely difficult for the burglar to enter the home, you discourage crime. The burglar will move on to a home where the pickings are easier.

Residential security is more important than we realize. Just ask the victim of a home that has been burglarized. The mother and wife responds, "I felt personally threatened and upset over the losses but more upset over the fact that our home was violated." The father and husband responds, "I'm happy my wife and daughter weren't home or they could have been hurt. Now I've got to call the police, my insurance agent, the repairman, and maybe an alarm company."

Too often people say, "It won't happen to me," "Our neighborhood never had a theft," "I sleep with a small gun by my bed," "I have a dog for protection," or "I don't need an alarm system." These are before-the-incident excuses. The cause of residential crime can be found in the individual's environment and lifestyle. Crime can be controlled and losses reduced by corrective human behavior. Physical security measures play an important role in preventing many crimes, but these measures are effective only if they are installed and used properly.

Alarms

Residential intrusion alarms are popular and installed frequently. The control panel (Underwriters Laboratories, UL, listed) also handles the fire alarm system. An audible horn distinguishes which system has gone off. The control panel should have an entrance/exit delay feature, which aids in the overall reduction of false alarms. Depending on the style of the home, any number of components can be used. However, keep in mind that only a total coverage system should be recommended and installed. Recent advances in IP technology allow homeowners, property owners, and place managers to operate their home intrusion detection systems remotely, giving added value to the security systems components installed on the property because they have become part of the property management function of the home.

Lighting

Improved lighting provides another residential security measure. Although some studies documented crime reduction after improved lighting systems were installed, these studies typically have not accounted for displacement effects. Even if individuals living in a residence reduce the likelihood of a burglary by better lighting, they may only be displacing the burglary to another, less lit area.

HOME SECURITY CHECKLIST

Massachusetts Crime Watch put together the following home security checklist, which deals with 35 security checkpoints:

Entrances

1. Are the doors of metal or solid wood construction?
2. Are door hinges protected from removal from outside?
3. Are there windows in the door or within 40 inches of the lock?
4. Are there auxiliary locks on the doors?
5. Are strikes and strike plates securely fastened?
6. If there are no windows in the door, is there a wide-angle viewer or voice intercommunications device?
7. Can the lock mechanism be reached through a mail slot, delivery port, or pet entrance at the doorway?
8. Is there a screen or storm door with an adequate lock?
9. Are all exterior entrances lighted?
10. Can entrances be observed from the street or public areas?

11. Does the porch or landscaping offer concealment from view from the street or public area?
12. If the door is a sliding glass door, is the sliding panel secured from being lifted out of the track?
13. Is a Charley bar or key-operated auxiliary lock used on the sliding glass door?
14. Is the sliding door mounted on the inside of the stationary panel?

Entrances from Garage and Basement

1. Are all entrances to living quarters from garage and basement of metal or solid wood construction?
2. Does the door from garage to living quarters have auxiliary locks for exterior entrance?
3. Does the door from basement to living quarters have an auxiliary lock operated from the living quarters' side?

Ground Floor Windows

1. Do all windows have key-operated locks or a method of pinning in addition to the regular lock?
2. Do all windows have screens or storm windows that lock from inside?
3. Do any windows open onto areas that may be hazardous or offer special risk of burglary?
4. Are exterior areas of windows free from concealing structure or landscaping?

Upper Floor and Windows

1. Do any upper floor windows open onto porch or garage roofs or roofs of adjoining buildings?
2. If so, are they secured as adequately as if they were at ground level?
3. Are trees and shrubbery kept trimmed back from upper floor windows?
4. Are ladders kept outside the house where they are accessible?

Basement Doors and Windows

1. Is there a door from the outside to the basement?
2. If so, is that door adequately secure for an exterior door?
3. Is the outside basement entrance lighted by exterior light?
4. Is the basement door concealed from the street or neighbors?
5. Are all basement windows secured against entry?

Garage Doors and Windows

1. Is the automobile entrance door to the garage equipped with a locking device?
2. Is the garage door kept closed and locked at all times?
3. Are garage windows secured adequately for ground floor windows?
4. Is the outside utility entrance to the garage as secure as required for any ground floor entrance?
5. Are all garage doors lighted on the outside?

Protecting Personal Property

A number of programs have been developed throughout the country that are geared to aid the citizen to reduce losses in the community. A number of these programs include the following:

1. **Operation Identification** is a program started in 1963 in Monterey Park, California. This program encourages citizens to engrave their personal property with a state driver's license number.
2. **Bicycle registration and antitheft program.** Some communities have started a mandatory registration of bicycles as well as an educational program. The educational program identifies poor quality locks used to secure bikes and provides instructions for properly securing a bike.
3. **Auto theft prevention** is another educational program, which is generally implemented

by the distribution of printed material and covered at community meetings. How many times have you seen a person keep the engine running while going into the store to buy milk? This is an example of giving the criminal an opportunity to commit a crime.

4. **Neighborhood Watch.** This program, initiated in 1971, encourages people to report suspicious circumstances in their neighborhoods to the police and familiarizes the citizens with crime prevention techniques to reduce criminal opportunity (see Chapter 10). Be alert for these suspicious signs:
   - A stranger entering a neighbor's house when the neighbor is not home
   - Unusual noises, like a scream, breaking glass, or an explosion
   - People, male or female, in your neighborhood who do not live there
   - Someone going door-to-door in your neighborhood, if he or she tries to open the doors or goes into the backyard, especially if a companion waits out front or a car follows close behind
   - Someone trying to force entry into a home, even if wearing a uniform
   - A person running, especially if carrying something of value

The person who sees anything suspicious is to call the police immediately. Give the responding officers a physical description of the person and license plate number of the car. Even if nothing is wrong, such alertness is appreciated. Remember, research has shown that the value of these citizen participation programs tends to wane over time without some periodic booster activities and part-time paid coordination to keep the program operating effectively and consistently.

1. **Security surveys.** Many police departments today have trained crime prevention officers who can provide security survey assistance to residents, enabling the citizen to better protect the family, home, and environment. Security professionals are also available as well as some auditors.
2. **Citizen patrols.** The citizen patrol can be viewed as part of the long historical tradition of vigilantism in this country, with all of the ambivalence present in that term. Presently, where their numbers are reported to be increasing in a number of suburban communities and cities across the country, citizen patrols are seen ideally as performing a relatively simple and narrowly defined role—to deter criminal activity by their presence. Their function should be that of a passive guard—to watch for criminal or suspicious activity and alert the police when they see it. Drawing on information that exists about current citizen groups, the advantages of patrols over other protective measures include that they:
   - Are relatively inexpensive.
   - Perform a surveillance function effectively.
   - Take advantage of existing behavior patterns.
   - Can improve an individual's ability to deal with crime.
   - Contribute to other desirable social goals related to neighborhood cohesiveness and the provision of a desirable alternative to less acceptable activity.

In practice, however, patrols exhibit serious shortcomings:

- The typical patrol is formed in response to a serious incident or heightened level of fear about crime. The ensuing pattern is cyclic: increased membership, success in reducing criminal activity at least in a specific area, boredom, decreasing membership, dissolution. As a result, patrols tend to be short-lived.
- The passive role of a patrol is difficult to maintain without at least a paid part-time coordinator.
- The police are reluctant to cooperate with a patrol and may even oppose it.
- The patrol may aggravate community tensions. The principal problems of patrols relate to their inability to sustain the narrow, anti-crime role they initially stress. They may be an effective temporary

measure to deal with criminal contagion in a particular area. Over the longer term, however, the inherent risks may outweigh the continued benefits. The proliferation of patrols in recent years is evidence that they fill a need, but it should be recognized that patrols are no substitute for adequate police protection.

Residential security can best be obtained by getting the facts on what you can do to secure the home, analyzing these facts, and arriving at a decision and implementing security measures.

TOP TEN SECURITY THREATS

Listed below are the top ten security threats to most communities (listed in no order of priority), followed by some questions that companies may use to assess their vulnerability to each threat.

1. **Staff Members and Staffing Agencies.** How confident are we that we are hiring bona fide people; do we carry out pre-employment screening? Do our suppliers and agencies carry out screening too? Who has access to our facilities?
2. **Loss of Data or Information.** How much of a concern are data breaches? Are we confident that our data, including those held by third parties, are secure? Are our systems secure, and who has access to them?
3. **Extremism and Terrorism.** How concerned are we by terrorist or extremist threats? Are we complacent, or have we carried out a reasonable assessment of the threats?
4. **Lack of Contingency or Business-continuity Planning.** Have we put contingency plans in place? Have we considered business continuity scenarios and communicated the plans to our employees?
5. **Physical Security.** How confident are we that our access controls and physical security measures are robust? Do they prevent social engineering and break-ins?
6. **Theft and Fraud.** Are we confident that we have preventative measures in place and processes to deal with events that may arise?
7. **Lack of Security Awareness.** Are employees aware of security? Do they change passwords, lock doors, and report issues?
8. **Storage and Disposal of Data and Information.** Are we confident that access to sensitive data is controlled? Is secure storage available and used? Do we destroy confidential waste in accordance with relevant standards, such as the BS8470: 2006 Secure Destruction of Confidential Materials guidelines?
9. **Lack of Training or Competency.** Do our staff members know what to do? Have they been trained in emergency procedures? Do they protect information?
10. **Regulatory Compliance.** Do we employ illegal workers? How do we investigate any infiltrations or allegations of noncompliance? Is a site compliant with required reporting and controls from Sarbanes-Oxley, HIPPA, ISO, UL, or other mandatory or voluntary standards?

THE AUDIT

Introduction

Compared to 20 years ago audits have become more popular and more demanding. They have become a very useful way to have an independent pair of eyes and ears reviewing your operation.

Below is an actual audit review checklist, currently used by a very familiar Fortune 500 corporation.

Exterior Access Controls

Objective: To determine whether sufficient controls are in place at this facility to deter and detect unauthorized access to:

1. External Utility Areas
2. Parking Facilities
3. Building Entrances

Approach: Review the latest version of the security manual related to exterior security.

1. Verify that facilities management has posted signs indicating property boundaries and entry restrictions.

2. Validate that critical utilities have been identified (generators, water systems, electrical stations, etc.), documented, and revalidated within the last 12 months. Determine if any required controls are implemented.
3. Verify that the minimum lighting requirements have been met and that no lights are burned out.
4. Verify that access from the parking structure is limited and secure. Determine if the area is well lit with concealment areas minimized using CPTED principles.
5. If it is a company-controlled site, determine if access to the parking structure is restricted to vehicles or drivers that are authorized and that there is an adequate number of handicap parking spaces.
6. If it is a company-controlled site, verify that there are physical deterrents (such as barriers or landscape techniques) that impede vehicular access to lobbies or other glassed areas of buildings where there is a concentration of people.
7. Verify that building access points below the third floor (grills, grates, manhole covers, utility tunnels, skylights, and roof vents, etc.) are secured to prevent entry into the building or damage to critical utilities, unless prohibited by local ordinances, codes, laws or regulations.
8. Verify that there is a clear line of sight maintained around the perimeter of the building.
9. All renovation and construction of any site security control centers must be reviewed and approved by the Director of Corporate Security.

Interior Access Controls

Objective: To determine whether appropriate access controls are in place within the facilities.

Approach: Review the latest version of the security manual related to building perimeters and interior security. Test for specific controls related to the various types of designated space.

- Perimeter doors
- Windows and exterior glass walls
- Internal space
- Restricted space
- Internal shared space
- Tenant restricted space
- Loading docks
- Lobbies and sensitive areas

1. Verify that all perimeter doors designed as entrances are constructed of heavy-duty material and are alarmed or monitored. Verify that all emergency exit doors are constructed of heavy-duty material and are alarmed. Determine if the door jambs, hinges, and locks are designed to resist forced entry.
2. Validate that windows on the ground floor cannot be opened more than 10 inches (25 cm).
3. Verify that all general use areas such as lobbies, elevators, and loading docks have a system to control access into interior space.
4. Validate that there are inconspicuous panic alarm devices in staffed lobbies that are monitored by Security or another constantly staffed workstation. Validate that staffed loading docks are equipped with panic alarm devices that are monitored by Security or another constantly staffed workstation. Verify that there is a documented response procedure and that the alarm devices are tested as required. In unstaffed lobbies and loading docks that are controlled by remote access doors, verify that there are monitoring devices to allow identification of an individual prior to allowing access to the building.
5. Validate that alarms (e.g., for doors, emergency exits, panic buttons, etc.) are tested to ensure they are operational and that the results are documented within the required time frame. Determine if corrective actions were taken and any deficiencies were documented.
6. Determine if the interior space is isolated from the public space (such as lobbies and public restrooms) with slab-to-slab construction techniques.

7. Determine if the restricted space has a supervised control access system with an audit trail, and that the audit trail is reviewed by management every 90 days. If cipher locks with audit function are used, validate that the combinations are changed every 90–95 days (or when employees change assignments).
8. Validate that no unauthorized individuals have access to terminals and printers. Determine if the contracts with tenants prohibit such access.
9. In locations where banking facilities (such as automated teller machines) exist, validate that there is a process for third-party monitoring for response to robberies and burglaries.
10. When a company shares space with a noncompany function, company employee offices and proprietary information must be secured when unattended.
11. CCTV digital recordings are saved for an appropriate period; refer to industry benchmarks for the appropriate recording retention length for your application (a 6-month period or longer; auditors want recorded data be available for at least 90 days).
12. Have e-mails been saved from managers that give his/her approval for specific employees to enter his specific space and has the approval been sought and given for specific employees to have access to a specific space?

Mail Services Security

Objective: To determine whether appropriate access controls are in place for the mail services area.

Approach: Review the latest version of the security manual related to mail services security.

1. Validate that access to the mailroom is restricted to authorized individuals only and a controlled access system is used.
2. Verify that doors and windows are equipped to protect against forced entry.
3. Verify that registered, certified, and confidential mail that is not delivered by the end of the workday is secured. This is not required if intrusion detection is installed that covers the entire mailroom area.
4. Verify that mailrooms that are multipurpose rooms (e.g., copier, fax, etc.), which serve as a mail delivery location or allow after-hours access, are equipped with lockable cabinets or lockable doors.
5. Verify that there are printed instructions regarding package identification posted in the mailrooms.
6. Learn whether there have been any past incidents at this site, or in this particular industry, where harm or risk has come to the place through the mail operation (e.g., bomb, threatening packages), and determine whether an off-site collection and mail screening facility is recommended.

Badges, Lock, and Key Controls

Objective: To determine whether badges, lock, and key program controls are adequate to deter and detect misuse. These requirements are only applicable to facilities where there is exclusive control of all keys providing access to space.

Approach: Review the latest version of the security manual related to lock and key controls.

1. Validate that master level keys (for example, grand master keys, building master keys, and floor master keys as defined in the security manual) are adequately controlled and only specific authorized people have MASTER access on their badges.
   a. Daily and/or shift accountability is maintained.
   b. Keys are restricted and controlled.
   c. If more than six access keys are available, site security manager documents approval every twelve months.
   d. Process to control access to master keys kept outside of security to allow landlords or fire/emergency response personnel access.
2. If Fireman Access Boxes, Knox Lock Boxes, or a Morse Watchmen Key Control or Badge Process is used:

a. Verify that these boxes are alarmed to a security control center or constantly staffed workstation.
b. Determine if duplicating hardware is secured when not in use.
c. Validate that all duplicate, blank, and unissued keys are properly secured when not in use.
d. Determine if key codes and pinning combinations are secured and available on a need-to-know basis.
e. If key operations are contracted, verify they are audited against requirements every 12 months

Access Controls and Badge Designs

Objective: To determine whether the processes and technology in support of physical access are operating effectively.

Approach: Review the latest version of the security manual related to access controls and badge designs.

1. Determine if badges are issued per requirements, for example:
   a. Documentation of management authorization for noncompany personnel was obtained prior the badge being issued.
   b. Proof of identity was obtained prior to a badge being issued to noncompany personnel.
   c. Temporary contractor badges are authorized by a manager, purchasing buyer, coordinator, or authorized predesignated contract company supervisor. Visitor identity (those requiring escort) must be validated by the person authorizing the visit.
   d. Badges are in compliance with the security manual design requirements (e.g., sealed, white photo background with a postage-guaranteed post office box return address on the reverse).
2. Validate that all badges have an expiration date in the database.
   a. Determine whether badges that are not returned on the due date (e.g., temporary or visitor badges) are deactivated.
   b. Determine whether badges reported as lost have immediate action taken to place the badge in lost status and whether the profiles are kept in the database for 6 months.
3. Validate that all hardware, badge stock, and other components of the badge process are secured when not in use.
4. Validate that user IDs are assigned to all operating personnel in compliance and authorization reviews are performed every 6 months.
5. Verify that an effective process is in place to remove employee access in a timely manner:
   a. Category manager reports are distributed to category managers every 90–95 days.
   b. Every 30 days Security must match database to the HR database.
   c. Process must be in place to deactivate lost badges or termed individuals within 24 hours.

Search Policy

Objective: Verify that the processes and technology in support of physical searches are operating effectively.

Approach: Review the latest version of the security manual related to search policy.

1. Validate that searches of personal effects, made without the employee's knowledge, are approved by management.
2. Validate that the policy for electronic searches (such as metal detectors, X-ray machines, and hand-held wands) has the approval of the senior site/location manager or senior location executive and the security manager. Determine if local laws have been followed.

Emergency Planning

Objective: To determine whether emergency plans have been established by senior location management that adequately address anticipated emergencies and catastrophes.

Approach: Review the latest version of the security manual related to emergency planning.

1. Verify that the senior location management emergency plan contains procedures for immediate response to emergencies.
2. Validate that the emergency plan addresses various types of emergencies (i.e., natural or humanmade disasters, threats or acts of violence against people or property, political/civil disturbances, and catastrophic events in close proximity to the site).
3. Validate that the security department, on behalf of the senior location manager, has reviewed the emergency plan within the last 6 months and updated the plan as needed.
4. Verify that a Crisis Management Team (CMT) has been designated and the team has met as a group once per year to conduct an exercise and training.
5. Validate that emergencies are promptly reported to Corporate Security.
6. Validate that the emergency plan is filed and that the senior location executive certifies that the plan is up to date.
7. Verify that requirements for the CMT are met: members have equipment such as a mobile phone, emergency plan, and aerial or site photo, and a room for the CMT is designated meeting the necessary requirements (emergency power, capability to receive national news, two telephones, workstation connectivity).

Reporting of Incidents

Objective: To determine whether there is an implemented process for the reporting of incidents to security.

Approach: Review the latest version of the security manual related to reporting significant incidents and responses.

1. Verify that a process exists to report all significant incidents (e.g., threats of violence, natural disasters, espionage, sabotage, thefts, and chemical spills) to Corporate Security.
2. Verify that referrals to law enforcement agencies are made when appropriate with the Director of Security notified.
3. Validate that the location has implemented the Security Incident Management System (SIMS) for reporting and classifying types of incidents and that relevant incidents are reported.

Investigations

Objective: To determine whether incidents are investigated, reported, and closed appropriately.

Approach: Review the latest version of the security manual related to investigations.

1. Validate that incidents have been reported to Corporate Security as appropriate and that knowledge of the investigation is limited to persons with a need to know.
2. Investigations involving government officials or law enforcement authorities must be referred to the Vice President of Corporate Security.
3. Validate that the use of covert monitoring (e.g., cameras and audio recorders) have required approvals.
4. Verify that any actions involving the sale or purchase of stolen property have the required approvals.

Emergency Response

Reference: Company Security Manual

Objective: In the event of an emergency, it is essential that employees know what to do in order to avoid danger and secure their safety. Proactive involvement in security emergency planning and emergency response will enhance employee well-being programs.

Approach:

1. Are emergency procedures developed for fire, first aid, pandemics, terrorist attacks, and any locally foreseeable disasters/emergencies? Does coordination exist between concerned parties, for example, local fire departments, law enforcement, security, location management, and so forth? Was

consideration given to the timeliness of response from community response services?
2. Were employees and site visitors made aware of emergency procedures?
3. Were emergency procedures developed and tested periodically to check effectiveness? Were practice evacuation fire drills conducted at least annually?
4. Did provisions exist for maintenance of adequate supplies and equipment?
5. Did a post-incident review process exist?
6. Did the designated emergency response organization have the appropriate training, have the capability to respond in a timely manner, and have the appropriate resources to handle emergencies? If emergency response teams are used, are all emergency response team members trained? Were emergency response equipment and vehicles maintained?

Fire and Life Safety

Objective: To determine if the location had implemented an effective process to detect, annunciate, and suppress fires to ensure life safety, and to comply with insurance company and regulatory requirements.

Approach: Review the fire/life safety program and related documentation.

1. **Building Design.** Do all new buildings and modifications to existing buildings meet local/national codes and the requirements of NFPA 101 or equivalent standard?
2. **Maintenance.** Are fire alarm systems, emergency lighting, fire dampers, automatic door closers, sprinkler and fire suppressant systems, fire extinguishers, and other similar safety features subject to inspection and maintenance as specified in local/national codes and insurance schedules?
3. **Contingency Measures.** Where there is a necessity to temporarily disable any building feature designed to protect users, the risks should be assessed and, where necessary, contingency measures introduced. Were there controls established to prevent unauthorized impairment of essential fire safety equipment?
4. **Life Safety and Fire Prevention.** Was there a fire prevention program implemented to address work practices that minimize the likelihood and consequences of fire?
5. **Testing the Effectiveness of Arrangements.** Were buildings subjected to a required periodic practice fire evacuation to assess the effectiveness of arrangements, familiarize occupants with requirements, and identify improvements?
6. **Fire Prevention.** Are fire wardens in place and are fire evacuation drills conducted annually?

REFERENCES

[1] Momboisse RM. Industrial security for strikes, riots and disasters. Springfield, IL: Charles C Thomas; 1968.
[2] Kingsbury A. Introduction to security and crime prevention surveys. Springfield, IL: Charles C Thomas; 1973.
[3] Washington Crime Watch. Crime prevention training manual. Security survey section, p. 8.
[4] Massachusetts Crime Watch. Home security test booklet. Waltham, MA: LEAA; 1980.
[5] LaFaver D. The home security book. ; 16. Shell Oil Company, p. 6. Permission obtained from Norman Mortell, BA, Director of Operations : Agenda Security Services; May 2010.
[6] www.tssbulletproof.com.
[7] www.pacificbulletproof.com.

APPENDIX 3.A. SITE SURVEY AND RISK ASSESSMENT*

Victor Harold and John O'Rourke, CPP

Crime prevention, or lessening the potential for crime, begins with a major in-depth security analysis of the business or facility. A survey of the interior and exterior will point out security deficiencies and potential for intrusion or the probability that a crime will occur at that spot.

After the survey, an appraisal and recommendation for action should be immediately undertaken.

*Reprinted with permission of Harold, V., How to stop theft in your business. Updated by John O'Rourke, CPP, 2011.

A timetable for implementing the recommendations should be originated and strictly followed.

It is possible the site survey is beyond the ability of most business managements. If it is, you are advised to obtain the services of a qualified security professional.

You are also urged to have this service performed immediately. Consider the vulnerability of your business to imminent criminal intrusion. Many burglarized companies as well as those that were victimized by white collar crime have suffered irreversible losses, slowdown, and even shutdown.

This appendix broadly points out the external and internal geographical areas that may require immediate and long-term consideration to help prevent criminal breach of the premises.

1. Can you obtain a neighborhood crime statistics report from the local police?
2. Can you determine if there has been any labor unrest in the area?
3. Can you obtain a report that details the extent of damage a labor unrest may have had on a firm in the area?
4. What is the prevalent type of damage done to companies during a labor unrest in the area?
5. Has your company ever been victimized by the labor unrests of other companies in the area?
6. Have prior tenants or owners of your facility ever reported a criminal incident?
7. What types of crimes are the most prevalent in the area? List by percentage and frequency.
8. Is your facility very visible from the local roads?
9. Is there easy access by emergency vehicles to your building from the local roads?
10. Do you have a chart showing the frequency of police patrols in the area?
11. Do you know how long it would take an emergency or police vehicle to reach your facility?
12. Do you have an evaluation of your building's roof and doors that details the length of time it will take for a break-in to be successful?
13. Do you have an evaluation of the safes, locks, and other devices to ascertain how long they can delay being opened?
14. If you require separate storage of high-risk or valuable items, are they placed in a high security area that may discourage intrusion?
15. Is personnel movement into and within the building controlled?
16. Have the door and window hardware been evaluated for ease of entry?
17. Have window openings been secured? (Check with local fire department codes.)
18. Are important files and computer operations secured in an area that prohibits unauthorized entry?
19. Is the lighting sufficient throughout all work areas?
20. Are vent and roof access panels and doors wired and latched to prevent intrusion?
21. Have you prevented external access to the locker rooms and vending and lounge areas?
22. Are the financial handling areas separate and secure?
23. Do you keep your safe's contents and the combinations and the controls needed to maintain security confidential?
24. Are the removable panels and grates in which a person or inventory may be concealed periodically removed and checked?
25. Can these panels and grates be more securely fastened without compromising the item to which they are installed?
26. Will you require police, fire department, or building department approval to more securely fasten those panels and grates?
27. Are the incoming electrical lines well secured and vandal free?
28. Are the panels on all electrical items fastened?
29. Are the electrical power grids, panels, backup, power supplies, etc., kept in a separate locked area?
30. Have you conducted a walk around the property to see if trees, hedges, walls, and fences can hide a person or goods?

31. Have you considered immediate action to correct?
32. If some visibility obstructions exist, are you taking steps to correct?
33. To prevent inventory from going out with the trash, are you keeping a secure trash collection area?
34. To prevent roof access, are trees and their branches next to buildings removed?
35. Are ladders kept secure?
36. Are you aware that noisy equipment can mask unauthorized entry?
37. Are all exterior building entry points alarmed?
38. Are you aware that certain internal and external conditions may affect the alarm?
39. Is there a log of alarm malfunctions and their causes?
40. Have all the causes of alarm malfunction been remedied?
41. Is there an alarm listing and maintenance schedule?
42. Has the police or security company's response to an alarm been tested?
43. Are key management personnel frequently tested on alarm use?
44. Have key personnel been given specific alarm control assignments, including alarm opening, closing, checkout procedures, and accountability?
45. Are there clearly established money handling procedures to follow for safeguarding cash deposits, etc.?
46. Do you have a policy for reporting thefts other than security breaches? (Anonymously, if you think it is best.)
47. Are office machines, shop equipment, and other easily movable items marked for identification purposes?
48. Are vendors, salespeople, and repair persons logged in and out and, when necessary, given visitor's passes?
49. Are the employees frequently updated on security procedures?
50. Are you keeping a file of security deficiencies and a schedule for correction?

APPENDIX 3.B. PHYSICAL SECURITY SURVEY*

Victor Harold and John O'Rourke, CPP

EXTERIOR PHYSICAL CHARACTERISTICS: PERIMETER GROUNDS

1. Is the fence strong and in good repair?
2. Is the fence height (a minimum of 8 feet excluding a 1 foot top guard of 3 strands of barbed wire) designed so that an intruder cannot climb over it?
3. Is the design of the fence from the building designed so that an intruder cannot climb over it?
4. Are boxes or other materials placed at a safe distance from the fence?
5. Are there weeds or trash adjoining the building that should be removed?
6. Are stock, crates, or merchandise allowed to be piled near the building?
7. Is there a clear area on both sides of the fence?
8. Are unsecured overpasses or subterranean passageways near the fence?
9. Are the fence gates solid and in good condition?
10. Are the fence gates properly locked?
11. Are the fence gate hinges secure and nonremovable?
12. What types of locks and chains are used to secure the gates?
13. Have unnecessary gates been eliminated?
14. Do you regularly check those gates that are locked?
15. Are blind alleys near buildings protected?
16. Are fire escapes and exits designed for quick exit but difficult entry?
17. Is the perimeter reinforced by protective lighting?

* Reprinted with permission of Victor Harold and updated by John O'Rourke, CPP, 2011.

18. Has shrubbery near windows, doors, gates, garages, and access roads been kept to a minimum?
19. What are the physical boundaries of the residence's grounds?
20. Does lighting illuminate all roads?
21. Is there a procedure to identify vendors, subcontractors, and visitors before entrance to the gate?
22. Is proper signage in place?

Exterior Doors

1. Are all doors strong and formidable?
2. Are all door hinge pins located on the inside?
3. Are all door hinges installed so that it would be impossible to remove the closed door(s) without seriously damaging the door or jam?
4. Are all door frames well constructed and in good condition?
5. Are the exterior locks double cylinder, dead bolts, or jimmy proof?
6. Can the breaking of glass or a door panel allow the person to open the door?
7. Are all locks working properly?
8. Are all doors properly secured or reinforced?
9. Are all unused doors secured and alarmed?
10. Are the keys in possession of authorized personnel?
11. Are keys issued only to personnel who actually need them?
12. Are the padlocks, chains, and hasps case hardened?
13. Are the hasps installed so that the screws cannot be removed?

Exterior Windows

1. Are nonessential windows bricked up or protected with steel mesh or iron bars?
2. Are all windows within 14 feet of the ground equipped with protective coverings?
3. Are the bars or screens mounted securely?
4. Do those windows with locks have locks designed and located so they cannot be reached or opened by breaking the glass?
5. Are small or expensive items left in windows overnight?
6. Is security glass used in any of these windows?
7. Are windows located under loading docks or similar structures protected?
8. Can windows be removed without breaking them?
9. Do all vents and similar openings have a gross area of 1 square foot or more secured with protective coverings?
10. Are windows connected to an alarm system adequately protected?
11. Are windows not secured by bars or alarms kept locked or otherwise protected?
12. Have windows (doors) been reinforced with Lexan?
13. Are all windows properly equipped with locks, reinforced glass, or decorative protective bars or sturdy shutters?
14. Are unused windows permanently closed?

Other Openings

1. Do you have a lock on manholes that give direct access to your building or to a door that a burglar could easily open?
2. Have you permanently closed manholes or similar openings that are no longer used?
3. Are your sidewalk doors or grates locked properly and secured?
4. Are your sidewalk doors or grates securely in place so that the entire frame cannot be pried open?
5. Are your accessible skylights protected with bars and/or an intrusion alarm?
6. Did you eliminate unused skylights, which are an invitation to burglary?
7. Are exposed roof hatches properly secured?
8. Are fan openings or ventilator shafts protected?
9. Does a service tunnel or sewer connect to the building?

10. Do fire escapes comply with city and state fire regulations?
11. Are your fire exits or escapes designed so that a person can leave easily but would have difficulty entering?
12. Do fire exit doors have a portable alarm mounted, to communicate if the door is opened, or is it hooked up to the intrusion alarm?
13. Can entrance be gained from an adjoining building?

Exterior Lighting

1. Is the lighting adequate to illuminate critical areas (alleys, fire escapes, ground level windows)?
2. How many foot-candles is the lighting on horizontal at ground level?
3. Is there sufficient illumination over entrances?
4. Are the perimeter areas lighted to assist police surveillance of the area?
5. Are the protective lighting system and the working lighting system on the same line?
6. Is there an auxiliary system that has been tested?
7. Is there an auxiliary power source for protective lighting?
8. Is the auxiliary system designed to go into operation automatically when needed?
9. Are the protective lights controlled automatically by a timer or photocells or is it manually operated?
10. What hours is this lighting used?
11. Does it use a switch box(es) or is it automatically time secured?
12. Can protective lights be compromised easily (e.g., unscrewing of bulbs)?
13. What type of lights are installed around the property?
14. Are they cost effective?
15. Are the fixtures vandal proof?
16. Is there a glare factor?
17. Is there an even distribution of light?

Interior Physical Characteristics

1. Name of the site.
2. Address.
3. Full name and exact title of the administrative officer.
4. Telephone number.
5. Name of the surveying officer.
6. Full name and exact title of the security liaison.
7. Describe the security problem at this site.
8. What is the general purpose of the site?
9. What is the range of hours in use?
10. Which hours and days represent high-activity use?
11. How many people have access to the site?
12. Is the site normally open to the public?
13. List the number of rooms occupied by the various departments and offices.
14. Who does maintenance?
15. On what schedule does maintenance operate?
16. List the estimated dollar value of equipment and property in each department or office.
17. What area has the highest dollar value?
18. What area contains the most sensitive material?

Interior Lighting

1. Is there a backup system for emergency lights?
2. Is the lighting provided during the day adequate for security purposes?
3. Is the lighting at night adequate for security purposes?
4. Is the night lighting sufficient for surveillance by the local police department?

Doors

1. Are doors constructed of a sturdy and solid material?
2. Are doors limited to the essential minimum?
3. Are outside door hinge pins spot welded or bradded to prevent removal?

4. Are those hinges installed on the inward side of the door?
5. Is there at least one lock on each outer door?
6. Is each door equipped with a locking device?

Offices

1. Can entrances be reduced without loss of efficiency?
2. Are office doors locked when unattended for long periods?
3. Does the receptionist desk have a clear view of the entrance, stairs, and elevators?
4. Are maintenance people and visitors required to show identification to the receptionist?
5. Are desks and files locked when the office is left unattended?
6. Are items of value left on desks or in an unsecured manner?
7. Are all computers bolted down?
8. Are floors free of projections, cracks, and debris?
9. During normal working hours, is the storage facility kept locked when not in use?
10. How many people have keys to this door?

Keys

1. How many keys are issued? How many master keys?
2. Is there a key control system?
3. What is the basis of issuance of keys?
4. Is an adequate log maintained of all keys issued?
5. Are key holders ever allowed to duplicate keys?
6. Are keys marked "Do Not Duplicate"?
7. If master key(s) are used, are they devoid of markings identifying them as such?
8. Are losses or thefts of key(s) promptly reported to security?
9. Who (name and title) is responsible for issuing and replacing keys?
10. When was the last visual key audit made (to ensure they had not been loaned, lost, or stolen)?
11. Were all the keys accounted for? (If not, how many were missing? How often do you conduct visual audits?)
12. Are duplicate keys stored in a secure place? Where?
13. Are keys returned when an employee resigns, is discharged, or is suspended? (If not, why not?)

Locks

1. Are all entrances equipped with secure locking devices?
2. Are they always locked when not in active use? (If not, why not?)
3. Is the lock designed or the frame built so that the door cannot be forced by spreading the frame?
4. Are all locks in working order?
5. Are the screws holding the locks firmly in place?
6. Is the bolt protected or constructed so that it cannot be cut?
7. Are locks' combinations changed or rotated immediately on resignation, discharge, or suspension of an employee having possession of a master key(s)? If not, why not?
8. Are locks changed once a year regardless of transfers or known violations of security? If not, why not?
9. When was the last time the locks were changed?

Petty Cash

1. How much petty cash is kept?
2. Are funds kept to a minimum?
3. Where is petty cash secured?
4. Are blank checks also stored there?
5. Are checks presigned?
6. Is the accounting system adequate to prevent loss or pilferage of funds accessible to unauthorized persons at any time?
7. Are funds kept overnight in a safe, locked desk, or file cabinet?
8. Is this storage area secure?

9. Are locks in the storage area replaced when keys are lost, missing, or stolen?
10. How many people handle petty cash?

Safes

1. What methods are used to protect the safe combination?
2. Are combinations changed or rotated immediately on resignation, discharge, or suspension of an employee having possession of the combination? If not, why not?
3. Is your safe approved by UL?
4. Is your safe designed for burglary protection as well as fire protection?
5. Where is (are) the safe(s) located?
6. Is it well lit at night?
7. Can it be seen from outside?
8. Do you keep money in your safe?
9. Do you keep cash at a minimum by banking regularly?
10. Do you use care in working the combination so that it is not observed?
11. Do you spin the dial rather than leaving it on "day lock"?
12. Do you have a policy of making certain that the safe is properly secured and the room, door(s), and windows are locked; nightlight(s) is on; and no one is hidden inside?
13. Is your safe secured to the floor or wall?
14. Are combinations changed at least every 6 months? If not, when was the last time?
15. Do you have a protective theft alarm? If yes, is it local or central?
16. When was the system tested last?

Inventory Control

1. When was the last time an inventory of business equipment was made, listing serial numbers and descriptions?
2. Were any items missing or unaccounted for?
3. Are all computers and similar equipment bolted down or otherwise secured?
4. Has the firm marked all its business equipment?
5. Is all expensive business equipment stored in a security cabinet or room?

APPENDIX 3.C. PLANT SECURITY CHECKLIST*

Victor Harold and John O'Rourke, CPP

1. Have you obtained a list of certified protection professionals (CPP) from the American Society for Industrial Security International (Arlington, Virginia)?
2. Have you assigned a senior executive (CSO) to act as liaison with the security consultant?
3. Have you assessed overall plant vulnerability to a variety of risks?
4. Have you checked with local police agencies about the incidence of vandalism, damage, reported internal losses, burglaries, and other crimes in the vicinity?
5. Have you checked with fire officials about the local incidence and type of fires and extent of losses?
6. Do you do periodic reviews of the plant security system, especially with a view toward effectiveness?
7. Do you periodically review the efficiency and willingness of the assigned security executive to carry out the function?
8. In many situations, the cost of security is far greater than the actual or expected loss. Have your circumstances been analyzed for cost-effectiveness?
9. Do you maintain a list of security regulations? Is it properly posted? Is it periodically reviewed?
10. Are you certain there has been no negligence in the guard force?
11. How often do you review the methods used to screen new employees, and are you certain screening is done?
12. Is there a policy to prevent laxity and indiscriminate use of badges and passes?
13. On termination of employment of a senior executive, are locks, codes, and passwords changed and badges deleted?

*Reprinted with permission of Victor Harold and updated by John O'Rourke, CPP, 2011.

14. Have you trained line supervisors to daily check the plant's interior and exterior physical condition?
15. Do you tell your plant engineers to daily check critical utility areas, such as sewers, telephone, water, and electricity, for damage?
16. If security equipment is to be installed, has the installation plan been approved by a qualified group, such as the fire department, architect, police department, or engineer?
17. Has there been a recent security evaluation of hardware, containers, fire control equipment, safety items, locks, and bars?
18. Do you have a daily inspection of interior and exterior intrusion detection systems, fire systems, and sprinkler systems?
19. Do you daily test and examine your alarm system for proper operation?
20. Is your alarm system of the divided type; that is, can small segments be disconnected from the still operational main system?
21. Do you have a security communication network? Are all parts operating?
22. If you use CCTV and cameras, are all stations functioning well?
23. When purchasing new equipment, is the suitability and reliability of the items checked out by a dependable group?
24. Do you have a study showing that your security measures can generate a return on investment because losses are avoided and assets are recovered?
25. Has a thorough security survey identified various probable events, such as pilferage or white collar crime, to which the company is vulnerable?
26. Can an approximate dollar amount be placed on each factor?
27. Will the survey estimate the cost versus benefit ratio of attempting to correct any security infringement?
28. Does the security survey or audit answer the following:
    a. What is the possibility of a specific occurrence?
    b. What is the probability of a specific occurrence?
    c. What set of circumstances has to be in place for a situation to happen?
    d. If a problem occurs, how much will it cost to correct and restore?
    e. Is there any personal risk to people?
    f. If we do not install a security system, can we handle most situations on our own?
    g. What is the correct security level required to accomplish the mission?
29. Do you minimize contact between employees and nonemployees (as much as possible)?
30. Do you keep a record of which employees have keys to specific areas?
31. Are locks changed regularly?
32. Are doors double or triple locked?
33. Are external signs posted stating that alarm systems are in operation?
34. Because the roof is a weak spot, has it been properly protected from intrusion, such as with sensitive sonic alarms or microwave?
35. Have perimeter entrances been minimized to prevent accessibility by key?
36. Have you determined whether you need a badge or employee pass identification system?
37. Are your employees trained to challenge an unrecognized visitor or non-pass-wearing person?
38. Are outside service vendors escorted to the job site? Periodically checked or stayed with? Escorted out?
39. Do you retain a security consultant to annually review physical security needs and update security devices?
40. Do your employees know you will prosecute theft offenders?
41. Have you requested that your alarm agency notify you if the premises have been visited during unusual hours by an employee with a key?
42. Are office keys given only to those who need access?

43. Do you have a record of which key was given to whom?
44. Do you collect keys immediately from discharged employees?
45. Do you change the locks of areas in which discharged employees had access?
46. Are keys marked with "Do Not Duplicate" logos?
47. Are serial numbers ground off keys to prevent duplication by number?
48. Is a responsible executive in charge of key distribution?
49. Are spare keys kept in a secure cabinet?
50. Are duplicate records kept, indicating key distribution and date and time issued?
51. Can your telephones be locked to prevent unauthorized after-hours use?
52. Do you have a locksmith who periodically checks all lock operations?
53. Can personal items be secured in a locked desk drawer?
54. Are important papers kept in a double-locked and fireproof file?
55. When filing cabinets are unlocked for use, are keys removed and secured?
56. Are office machines bolted down and locked?
57. Are your office machines and plant equipment marked for identification?
58. Are the serial numbers of office and plant equipment recorded, duplicated, and secured?
59. Are briefcases with important documents left in a locked cabinet?
60. Are important papers removed from desks and locked when the area is not staffed?
61. When the building shuts down for the evening or weekend, are doors and windows checked by a manager?
62. Do service personnel from outside vendors have proper identification?
63. When shutting down for the evening, are potential hiding places checked?
64. Are the police and fire department numbers posted near each telephone?
65. Are safe combinations changed very frequently?
66. Are security officers' rounds checked every day?
67. Have you determined if a shredder is necessary?
68. Do you avoid keeping large sums of cash overnight?
69. Do visitors sign in?
70. If the employees wear passes, do your security people check them even if the wearers are familiar?
71. If you have a facility that requires constant security, do you escort your visitors?
72. Is a vigil kept on outside maintenance people?
73. If you have a sensitive security area, is access to it kept limited?
74. Is the security area marked with signs and color coded?
75. Do you need an area where sensitive talks take place?
76. Do you periodically check offices for signs of tampering, such as moved desks, paint marks, putty and other fillers used to seal holes, dust and scratch marks, and more?
77. Do you avoid discussing on the phone what you are going to do about your security situation?
78. Do you avoid ordering security sweeps and changes in security structure over the phone?
79. Do you test the integrity of the security service by ascertaining if they will plant a device?
80. Do your security officers observe the counter-surveillance people at work?
81. Are the items prone to tapping or targets for security intrusion sealed? Are the seals checked regularly?
82. If a bug is found, do you continue to search for more?
83. Are all entry places alarmed?
84. Do you have a locker area for employees' personal use? Is the facility kept secure?
85. Are your security officers routinely given polygraphs, fingerprinted, and vetted?

APPENDIX 3.D. SECURITY OFFICERS CHECKLIST*

Victor Harold and John O'Rourke, CPP

1. Have you determined whether or not you have limited security requirements?
2. If you have determined that your security needs are complex, have you talked about your needs to a select group of trustworthy agencies?
3. If your security needs are simple, are you aware that it is time consuming and a waste of productivity to obtain a wide variety of competitive bids?
4. Have you checked with a local law enforcement official for recommendations?
5. Have you checked with colleagues who use security services for recommendations?
6. If you are analyzing a security agency, have you requested information on the amount, type, and stipulations of their insurance coverage?
7. Have you requested information on the security agency's clients, the names of current customers, and the length of time the account has been with the agency?
8. Have you requested information on the agency's financial status?
9. Is the agency willing to reveal security officer training techniques?
10. Does the agency have security officer incentive programs?
11. Does the agency have a career program for its security officers?
12. Do the guards meet educational and criminal background checks?
13. Has the agency a set of standards to which security officers are held? What are they?
14. Have you reviewed the credentials of the senior executives of the guard service company?
15. Will your account have a representative assigned who is from the highest level of management?
16. Will the agency you select have the capabilities to offer other services, such as investigations, disaster planning, executive protection, employee screening, and polygraph testing?
17. Have you determined if the agency you are selecting has a union affiliation? Which one?
18. Will there be a union conflict if your employees go on strike?
19. Have you visited the agency's local office?
20. Have you discussed prior clients and why they no longer are clients?
21. Have you visited current accounts and talked to management?
22. In the contractual arrangement with the guard company, have you avoided too much control over their employees?
23. Have you double-checked the insurance liability of the agency?
24. Does the contract with the guard company assure that it is an independent contractor, relieving your firm of joint employer liability?
25. Have you reviewed the contract's provisions for replacing unsatisfactory guards and terminating the contract?
26. Does the contract guarantee costs?
27. Does the contract contain penalties for nonperformance or poor performance?
28. Is there an agreement by the guard company to refrain from doing business with a competitive company?
29. Have you assigned a senior person to monitor security services to determine that standards are being met and the agency's contractual obligations are being fulfilled?
30. If your plant is paying for guard services, have you discussed wages and job-related expenses, such as travel, holidays, and supervisors?
31. Have you discussed any special training required to accomplish the assignment, such as firearms, CPR, fire safety, and first aid?

*Reprinted with permission of Victor Harold and updated by John O'Rourke, CPP, 2011.

32. If your situation requires a formal presentation and contract, have the documents been reviewed by your legal counsel and insurance company?
33. Have you reviewed provisions for contract terminations?

APPENDIX 3.E. OFFICE SECURITY CHECKLIST

Victor Harold and John O'Rourke, CPP

The UCLA Campus Police Department put together the following office security checklist, which deals with 30 security points pertaining to operational procedures as well as physical characteristics.

1. Do you restrict office keys to those who actually need them?
2. Do you keep complete, up-to-date records of the disposition of all office keys?
3. Do you have adequate procedures for collecting keys from former employees?
4. Do you secure all computers and similar equipment with maximum security locks?
5. Do you restrict duplication of office keys, except for those specifically ordered by you in writing?
6. Do you require that all keys be marked "Do Not Duplicate" to prevent legitimate locksmiths from making copies without your knowledge?
7. Have you established a rule that keys must not be left unguarded on desks or cabinets; and do you enforce that rule?
8. Do you require that filing cabinet keys be removed from locks and placed in a secure location after opening cabinets in the morning?
9. Do you have procedures that prevent unauthorized personnel from reporting a "lost key" and receiving a "replacement"?
10. Is a responsible person in charge of issuing all keys?
11. Are all keys systematically stored in a secured wall cabinet either of your own design or from a commercial key control system?
12. Do you keep a record showing issuance and return of every key, including name of person, date, and time?
13. Do you use telephone locks to prevent unauthorized calls when the office is unattended?
14. Do you provide at least one lockable drawer in every secretary's desk to protect purses and other personal effects?
15. Do you have at least one filing cabinet secured with an auxiliary locking bar so that you can keep business secrets under better protection?
16. Do you record all equipment serial numbers and file them in a safe place to maintain correct identification in the event of theft or destruction by fire?
17. Do you shred all important papers or place them in a recycle bin for shredding?
18. Do you lock briefcases containing important papers in closets or lockers when not in use?
19. Do you insist on identification from repair personnel who come to do work in your office?
20. Do you deposit incoming checks and cash each day so that you do not keep large sums in the office overnight?
21. Do you clear all desks of important papers every night and place them in locked, fireproof safes or cabinets?
22. Do you frequently change the combination of your safe to prevent anyone from memorizing it or passing it on to a confederate?
23. When working alone in the office at night, do you set the front door lock to prevent anyone else from getting in?
24. Do you have the police and fire department telephone numbers posted and handy?
25. Do you check to see that no one remains behind hiding at night if you are the last to leave the office?
26. Are all windows, transoms, and ventilators properly protected?
27. Do you double-check to see that all windows and doors are securely locked before you leave?

28. Are all doors leading to the office secured by heavy-duty, double-cylinder dead bolt locks?
29. If your office is equipped with a burglar alarm system or protected by a guard service, do you make sure the alarm equipment is set properly each night?
30. Do you have a periodic security review made by a qualified security expert or locksmith?

APPENDIX 3.F. HOME SECURITY CHECKLIST*

Victor Harold and John O'Rourke, CPP

EXTERIOR

1. Do you have a burglar alarm?
2. Are there stickers on your windows and doors, stating that the property is alarmed?
3. Are bicycles, garden equipment, and other items kept indoors and locked?
4. Is your mailbox locked?
5. Are front and back doors kept lighted in the evening?
6. Are shrubs and trees trimmed low, below window level?
7. Do you arrange for mail and newspaper pickup or stop deliveries if you are not at home?
8. Is your grass kept mowed while you are away?
9. Is there a neighborhood watch program?
10. Do you place lights on timers or photocells if you go away?
11. Are police notified of your extended absence?

DOORS

1. Do all doors, especially to the garage and basement, close tightly?
2. Are all doors double locked?
3. Are overhead doors locked when not in use? Is there a track lock?
4. If padlocks are used, are they of high quality?
5. If hinges and hasps show, are the screws and hinge pins of the type that cannot easily be removed?
6. If your car is in the garage, are the doors locked and the keys removed?
7. Are the entrance doors solid core?
8. Is there a security plate in the lock area to prevent jimmying?
9. Are there peepholes or viewing windows in the entrance doors?
10. If the entry doors have glass, is the glass 40 or more inches from the lock?
11. Are sliding doors locked and has an anti-slide bar on the lower track, as well as bars on top of the doors, been installed to prevent lifting the door off the track?

WINDOWS

1. Are the window air conditioners bolted to prevent removal from the outside?
2. Can the basement windows be locked?
3. Do you use auxiliary pins and other locks on all windows?
4. If windows are kept open for ventilation, can they be locked in the open position?

GENERAL HOME SECURITY

1. Can all exterior doors be locked from the inside?
2. Are the locks on all exterior doors of the dead bolt type?
3. If a door or window is opened while you are home, will there be a warning sound or light?
4. When you retire or leave, do you check doors and windows to be certain they are locked?
5. When repair people and utility company representatives come to your door, do you request identification?
6. Can your basement door be locked to prevent entry into the house?

*Reprinted with permission of Victor Harold and updated by John O'Rourke, CPP, 2011.

7. Are extra house keys kept isolated or hidden?
8. Do you avoid indiscriminate handing out of duplicate keys?
9. If you park your car in a public lot, do you separate the car keys from the house keys?
10. Do you have an outside light that remains on all night?
11. Are all low-level windows that are easily accessible kept doubly secure with latches and bolts?
12. Have you installed window and door devices that audibly and visually indicate that a break-in is in progress or has occurred?
13. Are your skylights well secured, that is, not easily removed from the roof?
14. Are window air conditioners well installed and not removable from the outside?
15. Are your portable fire extinguishers kept in good condition?
16. Are they kept in easily accessible areas?
17. Are smoke and heat detectors installed near sleeping areas and on every level of the house?
18. Are the detectors tested frequently?
19. Are fire drills a regular routine with your family?
20. Do you have an emergency notification system to enable other households to know that a situation (medical, panic, robbery) is occurring?
21. If a suspicious vehicle is in the area, is a description and the license number noted?
22. If you go away, can you get a neighbor to park a spare car in your driveway?
23. Do you have a home safe for valuable items?
24. Should you have an alarm system survey to help determine your security and safety needs?

MISCELLANEOUS

1. Is valuable property inventoried, and is the list periodically updated and secured?
2. Is the list of serial numbers of those items that have been recorded kept off the premises?
3. Are valuable items marked with a scriber and an identifying number?
4. Are emergency telephone numbers memorized and prominently displayed near the telephone?
5. Do you avoid keeping cash in the house?
6. If you have weapons, are they secured?

APPENDIX 3.G. FIRE SAFETY INSPECTION

Michael A. Stroberger

The following inspection is designed to be the basis of a revised and property-specific inspection program. Some of the entries refer to functions performed with a "reasonable frequency." In reviewing your specific property or location, care should be taken to consider the nature of the structure, geographic location, intended use, and actual use. In many cases, functions that are best performed on a daily basis in one environment can be reasonably performed on a weekly or possibly monthly basis in a different environment.

In addition, note that every application is unique in some manner. As such, what might be prudent for one location, however seemingly similar, might be insufficient at another location. Although benchmarking of a similar program is highly recommended, this also should be seen as simply a basic guideline in the creation of a customized, location-specific program.

Some sections pose inspection inquiries that reference a large number of possible locations or items to be reviewed. One example would be the inspection of sprinkler heads. In designing the actual checklist for such an inspection, it is often desirable to break down the physical layout of the facility into reasonable and manageable zones. Identifying sets of sprinkler heads by the room in which they are installed allows the person performing the inspection to review them as a set and make comments in reference to that area of coverage. In cases such as fire doors, it might be reasonable to identify them with a location number, which could be included not only on the inspection form, but a numbered tag, on the hinge-side edge of the door, for later identification.

ADMINISTRATIVE AND PLANNING PHASE

1. Are copies of all locally enforced codes maintained on site for reference?
2. Does the facility meet requirements of locally enforced Building Code?
3. Does the facility meet requirements of locally enforced Fire Prevention Code?
4. Does the facility meet requirements of locally enforced Life Safety Code?
5. Does the facility have a written and appropriately distributed Fire Prevention and Response Plan? Is this plan known to all employees? Is training provided to those with defined responsibilities? Is all training documented and securely filed? Is the plan reviewed annually, updated as required, and redistributed?
6. Does the facility maintain a fire brigade? Is the fire brigade training documented and securely filed? Is the fire brigade training conducted in conjunction with the local fire department? Is the fire brigade composed of persons, or positions, that are present or represented at all times?
7. Are all inspection reports retained for a reasonable number of years, as defined by local codes, insurance requirements, or industry standards? Are inspection reports filed in a secure location?
8. Are all employees trained in basic fire prevention concepts and fire event response procedures? Is the content of this training consistent and reasonably inclusive? Is this training documented and securely filed? Is annual refresher training conducted? Is annual refresher training documented and securely filed?

General Physical Inspection Phase

1. Are all fire exit routes clearly marked? Are all exit routes unobstructed at all times? Are all exit routes and egress hardware items in compliance with the Americans with Disabilities Act requirements?
2. Are all fire doors and egress hardware items in proper working order?
3. Are service areas secured against unauthorized entry when not in use?
4. Are all areas free of loose or disorganized combustible items (such as rags or empty boxes)?
5. Are all storage areas well organized to allow ease of access in emergency situations?
6. Are flammable or combustible items properly stored to protect against accidental ignition?
7. Are flammable or combustible items properly stored to protect against unauthorized usage or tampering?
8. Are all fire lanes clearly marked? Are fire lanes maintained in an unobstructed condition at all times?
9. Are master keys available at all times for Fire Department use?
10. Are all electrical panels accessible at all times? Are all panels clearly marked to facilitate emergency power disconnection?
11. Are gas line shutoff valves accessible at all times?
12. Are all gas-operated pieces of equipment inspected for wear and damage with reasonable frequency? Are inspections documented and filed in a secure location?
13. Are all heat-generating devices (such as boilers, furnaces, and dryers) provided a reasonable clear zone, based on levels of heat output, where storage of any kind is prohibited?
14. Are all ducts inspected regularly and cleaned as required?
15. Is the use of extension cords discouraged in all areas?
16. Are all electrical cords and electrically operated items inspected for wear or damage with reasonable frequency? Are such inspections documented?
17. Are designated smoking areas clearly defined and at a proper minimum safe distance from any common or identified ignition threats? Are appropriate ash and cigarette receptacles available for use in these areas?

Extinguisher Inspection Phase

1. Have all extinguishers been inspected and serviced as required by a licensed vendor or trained technician within the past 12 months?
2. Are all extinguishers of a type appropriate for most probable types of fires in the immediate area?
3. Are specialty extinguishers available in those areas that would require them?
4. Are persons trained in the use of the extinguishers available in the areas where they are typically present? Is this training documented and filed in a secure location?
5. Are extinguishers inspected with reasonable frequency (daily, in most cases) to ensure that they are present and have not been tampered with or discharged? Is each extinguisher inspection fully documented and securely filed?

Stand Pipe, Fire Hose, and Control Valve Inspection Phase

1. Do tamper switches, linked to an alarm system, monitor all control valves?
2. Are all control valves inspected and tested annually by a licensed vendor or trained technician?
3. Are all stand pipes, control valves, and fire hoses accessible at all times?
4. Are fire hoses inspected, per manufacturer recommendations, for wear and decay?

Sprinkler System Inspection Phase

1. Are all flow switches inspected and tested annually by a licensed vendor or trained technician?
2. Are all sprinkler heads of a type appropriate for the location in which they are installed?
3. Are all sprinkler heads installed and maintained within the manufacturers' recommendations?
4. Are all sprinkler heads provided with a clear area of operation in compliance with the local Fire Code?
5. Does the sprinkler system have a pressure maintenance pump? If so, is this pump inspected and tested with reasonable frequency (weekly, in most cases) by a licensed vendor or trained technician?
6. Are all areas requiring sprinkler system coverage, per the local Fire Code, provided with such coverage?

Hazardous Materials Inspection Phase

1. Are proper warning placards utilized in areas of chemical storage and usage?
2. Is proper personal protective equipment (PPE) provided for initial response to fire and emergency situations related to any hazardous materials maintained or utilized on site? Is training provided in the use of this PPE? Is such training documented and filed in a secure location?
3. Is the Fire Department made aware of storage areas, use areas, and large arriving or departing shipments of hazardous materials?
4. Are all appropriate containment, standoff distance, and warning signs utilized in storage areas?
5. Is the MSDS on file and accessible 24/7?

Alarm System Inspection Phase

1. Is the system monitored by a licensed, offsite monitoring service?
2. Is the system inspected and tested annually by a licensed vendor or trained technician?
3. Is this inspection documented and filed in a secure location?
4. Is the area of coverage broken down into identified zones?
5. When activated, does the alarm system clearly identify the location of the potential fire?
6. Are audible alarms heard in all areas of a zone when activated? Is the system designed to warn adjacent zones, inclusive of floors above or below?

7. Are strobes visible in all areas of a zone when activated? Is the system designed to warn adjacent zones, inclusive of floors above or below?
8. Does the alarm system record activation and use history? For what length of time is this history retained?
9. Does the system's audible signal include a prerecorded advisory message? If so, does this message recommend a route or method of egress? If so, does this message advise against the use of elevators, if any are present?
10. Does the system automatically recall or drop elevators on activation? Are override keys available for Fire Department use?
11. Are detector types installed, as appropriate for the specific location of installation? If the intended use of a given area is altered, is the type of detector also reviewed and changed to match the updated intended use of that area?

SUMMARY

This is added for informational use only as it is not typically considered in the domain of the security professional.

In January 2003, the American Society for Industrial Security International came out with a set of General Security Risk Assessment Guidelines, which recommended that, when conducting a security survey or risk assessment of a complex, a company should consider the following seven points from their report:

1. Assets are people, property, intangible property, and information; identify the risks attached to each.
2. Conduct a cost/benefit analysis and explore the value of all benefits to be a accrued. Are the recommendations made affordable, feasible, available, practical, and state of the art?
3. Consider the risk, risk analysis, risk assessment, probability, and vulnerability to incidences.
4. Gather statistical data: material obtained from in house, material obtained from local and state police agencies, material from the FBI Uniform Crime Report database, and the type of incidents in similar complexes as well as the rating of the current Homeland Security color code.
5. Examine the frequency of events and what can be done to reduce and remove the overall threat.
6. Identify the assets; for example, a warehouse with a million-dollar inventory, 30 people have access and maybe more, alarm system control panel is a dialer non-UL that is 22 years old; or a museum with a 52-million-dollar inventory, four people have total access, and the 5-year-old fire and intrusion alarm at all points is tested monthly.
7. Reassess your complex annually.

Finally, we realize not all security personnel deal with fire safety and life safety issues, but some do.

APPENDIX 3.H. BULLET-RESISTANT GLAZING FOR A SECURE WORKPLACE

Michael A. Stroberger

Total Security Solutions offers a full line of bullet-resistant glass in acrylic, polycarbonate, and glass-clad polycarbonate. These products are available at UL protection Levels 1–8, providing protection ranging from 9 mm to a 12 gauge. These products are typically used in banks, credit unions, gas stations, and convenience stores but are appropriate for any business with cash on hand that wants to provide their employees with a secure work environment.

In addition to providing bullet-resistant products to glaziers and mill shops, Total Security Solutions provides custom milling and installation of secure barrier systems. We take pride in our ability to develop and install bullet-resistant architecture that fits the design of a customer-friendly workplace.

Typical materials used in construction or sold directly include:

- Interior/exterior transaction windows
- Bulletproof doors
- Ballistic counters

- Package passers
- Bullet-resistant barriers and framing
- Bullet-resistant transparencies and fiberglass

BULLET-RESISTANT FIBERGLASS WALL PANELS

These are used to provide bullet-resistant protection to the walls of corporate executive offices, boardrooms, conference rooms, lobbies, reception area counters, customer service counters, and safe rooms. This bullet-resistant fiberglass can be installed by the manufacturer or even by your general contractor. Once installed, this product will never be seen but will provide high-quality ballistic protection and peace of mind for years and years to come.

BULLET-RESISTANT DOORS

Along with protection for the walls and lobbies of your offices, there are a wide variety of doors to meet your needs, such as solid executive-style veneered doors to match existing doors; the only difference is that they will also offer bullet-resistant protection. Again, these doors provide invisible bullet-resistant protection, and nobody will know it is there. Aside from custom-made, executive-style office doors, normally there are full vision clear doors, half vision clear doors, plastic laminate no-vision doors, and bullet-resistant steel doors. All of these doors are prehung, so any contractor can install them within minutes.

BULLET-RESISTANT WINDOWS

Bullet-resistant windows come in a full range of windows that are custom built for the needs of each individual client. You can replace your office windows with bullet-resistant windows ranging from levels 1–5, or you can leave your existing windows in place and add a second bullet-resistant window behind the existing window in such a way that it will be virtually invisible to the general public and still add protection.

Bullet-Resistant Executive Office Products

- High-quality executive-style bullet-resistant doors
- Bullet-resistant wall armor to line all the walls of the office
- Bullet-resistant, custom-made windows to protect all existing window locations
- High-security electronic mag-locks to lock doors in the event of an attack

Bullet-Resistant Board Rooms or Conference Rooms

- High-quality, executive-style bullet-resistant doors
- Bullet-resistant wall armor to line all the walls of the conference room or board room
- Bullet-resistant, custom-made windows to protect all existing window locations
- High-security electronic mag-locks to lock door in the event of an attack
- Bullet-resistant transaction or reception area
- Bullet-resistant transaction window systems
- Package exchange units
- Bullet-resistant reception door with electric strike
- Bullet-resistant fiberglass for reception counter die wall
- Stainless steel deal trays for small transactions

Residential High-Level Security for Corporate Executives

- Provide bullet-resistant protection to point of entry (garage, front doors, front windows, etc.)
- Build safe room including walls, doors, windows, and high-security locksets
- Convert closet into a high-level safe room
- Convert master bedroom into a high-level safe room (add invisible bullet-resistant protection to all walls, doors, and windows)

Finally, be advised that there are standards that apply to these installations and the products.

APPENDIX 3.I. WINDOW FILM

Michael A. Stroberger

Window film is not bulletproof and there is *no* film product out there that is. However, window film can be resistant to small arms and shotguns, and Lumar window film products have a bomb blast proof film product.

Window film comes in four categories:

1. Security or safety film
2. Decorative or safety film
3. Anti-graffiti film
4. Solar film

One benefit of security or safety film is that when an outer pane of glass breaks, the inner pane will remain intact. It is used to protect retail, commercial, and residential buildings as well as other types of window structures from flying glass due to earthquakes, windstorms, attacks, vandalism, theft, and accidents.

Decorative film makes glass surfaces clear and visible, enhances safety in public spaces, and allows you to customize your space with a corporate logo.

Anti-graffiti window film is a protective film that helps prevent scribing on or defacing of your base surface. The film is easily peeled off and replaced, eliminating graffiti and the replacement cost of glass.

Solar film has many benefits: it reflects and absorbs heat and light, increases energy efficiency, reduces HVAC cost, protects furniture and carpets, and provides greater temperature stability. Below are a list of websites in the event you seek additional information.

www.iwfa.com
www.extremewindowsolutions.ca
www.acelaminate.com
www.securityfilm.biz/index.htm

CHAPTER

4

Approaches to Physical Security*

Richard Gigliotti, Ronald Jason

Protection of one's person and possessions is natural and universally accepted. Unfortunately, there are those who have made it their objective to deprive some of us of one or both of these. In the battle against the criminal element, our resourcefulness in designing and developing more and better methods of protecting our life, property, and livelihood has been unbounded. No system, however, can be made completely secure. Any system conceived can be defeated.

In other words, no physical protection system is 100% defeat-proof. If it can be designed to eliminate most threats, it will have its weak links, for example, with a perimeter fence or an alarm system. In any event, if a system cannot fully protect against a threat, it must at a minimum offer enough protection to delay the threat until the system can be upgraded, at least temporarily, to the point at which the threat can be defeated (e.g., the arrival of local law enforcement authorities or on-site guard force, the implementation of contingency measures such as additional physical barriers, or the release of noxious gases).

Maximum security is a concept. Physical barriers, alarm systems, guard forces, and all the other components of a security system do not individually achieve maximum security. The parts of the system cannot realize the ultimate aim unless they are combined in the right proportions.

LEVELS OF PHYSICAL SECURITY

How would one categorize a particular security system? Would one consider protection minimum, medium, or maximum, and what criteria would be used in making this determination? Would a facility be compared to a prison, nuclear reactor, department store, or the average American home? While the initial question may appear to be answered easily, arriving at an intelligent and impartial assessment becomes much more difficult simply because there are no known universally accepted standards by which the security professional may evaluate a security system.

This lack of standards often deludes responsible individuals into believing that the protection they provide (or are paying for) is of a higher level than is actually the case. Because of the confusion and lack of cohesive opinion on the subject, this chapter considers the following five levels of security systems (also see Figure 4-1):

Level 1: minimum security
Level 2: low-level security
Level 3: medium security
Level 4: high-level security
Level 5: maximum security

*Originally from Security design for maximum protection. Boston: Butterworth-Heinemann, 2000. Updated by the editor, Elsevier, 2011.

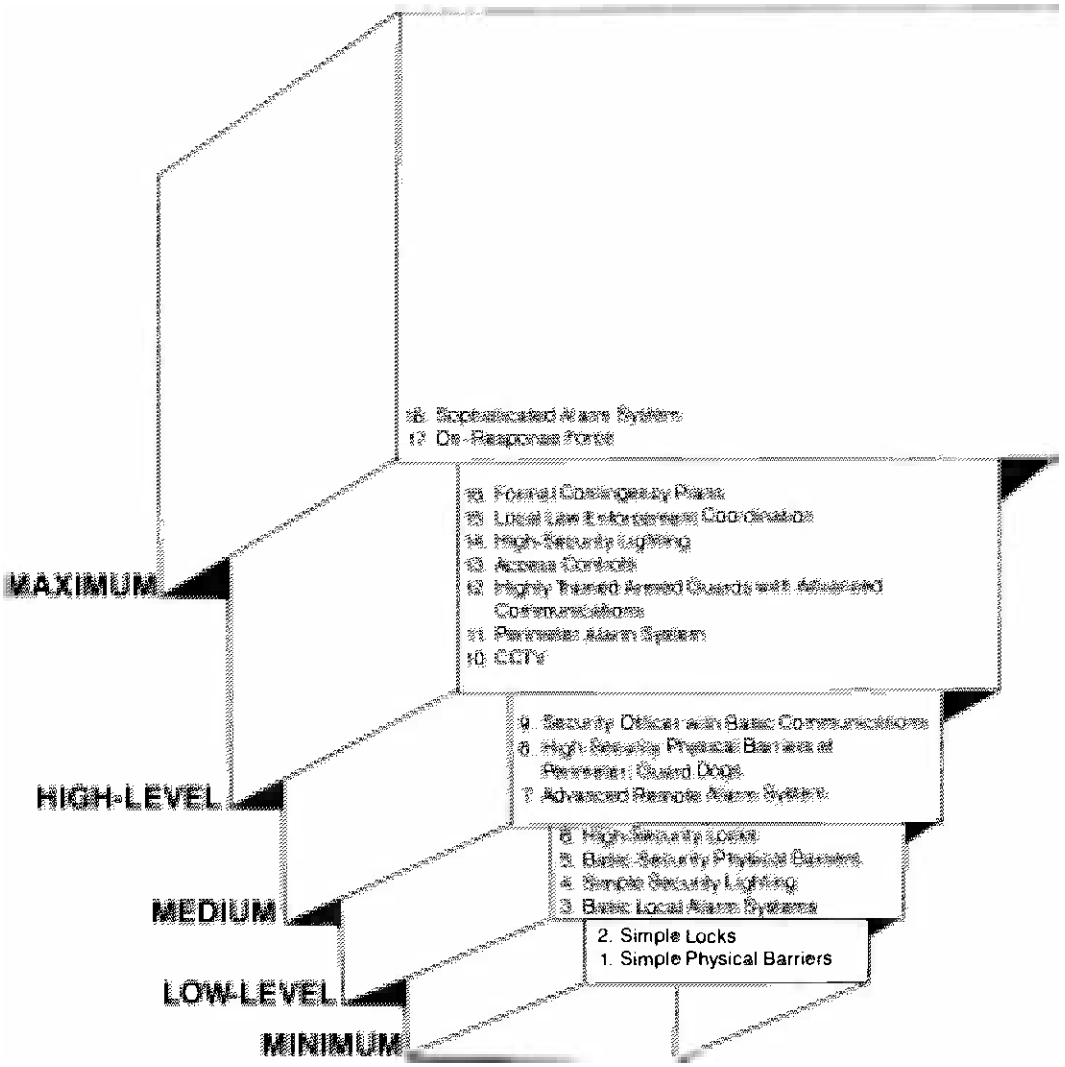


FIGURE 4-1 The level of physical security. *(Reprinted with permission from* Security Management.*)*

Minimum Security

Such a system would be designed to *impede* some unauthorized external activity. Unauthorized external activity is defined as originating outside the scope of the security system and could range from simple intrusion to armed attack.

By virtue of this definition, a minimum-security system would consist of simple physical barriers such as regular doors and windows equipped with ordinary locks. The average American home is the best example of a site protected by a minimum-security system.

Low-Level Security

This refers to a system designed to *impede* and *detect* some unauthorized external activity. Once simple physical barriers and locks are in place, they can be supplemented with other barriers such as reinforced doors, window bars and

grates, high-security locks, a simple lighting system that could be nothing more elaborate than normal lighting over doors and windows, and a basic alarm system that would be an unmonitored device at the site of the intrusion that provides detection capability and local annunciation. Small retail stores, storage warehouses, and even older police stations are examples of sites that could be protected by low-level security systems.

Medium Security

A system of this type would be designed to *impede*, *detect*, and *assess* most unauthorized external activity and some unauthorized internal activity. Such activity could range from simple shoplifting to conspiracy to commit sabotage. When a system is upgraded to the medium level, those minimum- and low-level measures previously incorporated are augmented with impediment and detection capability as well as assessment capability. To reach the medium level of security, it is necessary to:

1. Incorporate an advanced intrusion alarm system that annunciates at a staffed remote location.
2. Establish a perimeter beyond the confines of the area being protected and provide high-security physical barriers such as penetration-resistant fences at least 8 feet high and topped with multiple strands of barbed wire or barbed tape at that perimeter, or use guard dogs in lieu of perimeter protection.
3. Use an unarmed guard (with basic training) equipped with the means for basic communication (e.g., commercial telephone) to offsite agencies.

Medium-security facilities might include bonded warehouses, large industrial manufacturing plants, some large retail outlets, and National Guard armories.

High-Level Security

A system of this sort would be designed to *impede*, *detect*, and *assess* most unauthorized *external* and *internal activity*. After those measures previously mentioned have been incorporated into the system, high-level security is realized with the addition of the following:

1. State-of-the-art equipment installed.
2. Closed-circuit television (CCTV) with state-of-the-art components and installation.
3. A perimeter alarm system, remotely monitored, at or near the high-security physical barriers.
4. High-security lighting, which at a minimum provides at least 0.02 foot-candles of light around the entire facility.
5. Highly trained armed guards or unarmed watch people who have been screened for employment and who are equipped with advanced means of communications, such as dedicated telephone lines, two-way radio links to police, and duress alarms.
6. Controls designed to restrict access to or within a facility to authorized personnel such as using access control and/or biometrics.
7. Formal plans prepared with the knowledge and cooperation of police dealing with their response and assistance in the event of specific contingencies at the protected site.
8. Varying degrees of coordination with local law enforcement authorities.
9. Annual assessment or security audits conducted.

Examples of high-level security sites include certain prisons, defense contractors, pharmaceutical companies, and sophisticated electronics manufacturers.

Maximum Security

Such a system is designed to *impede*, *detect*, *assess*, and *neutralize* all unauthorized *external* and *internal activity*. In addition to those measures already cited, it is characterized by:

1. A sophisticated, state-of-the-art alarm system too strong for defeat by a lone individual, remotely monitored in one or more protected locations, tamper-indicating with a backup source of power.

2. On-site response force of highly screened and trained individuals armed 24 hours a day, equipped for contingency operations, and dedicated to neutralizing or containing any threat against the protected facility until the arrival of off-site assistance.

The highest level of physical security protection will be found at nuclear facilities, some prisons, certain military bases and government special research sites, and some foreign embassies.

To upgrade a security system to the next highest level, all criteria for that level must be met (see Figure 4-1). Remember that individual criteria from a higher level can be met without upgrading the total system. For example, if a medium-security facility institutes access controls and installs a CCTV system, the overall level of security has not been upgraded to a high level. In reality, what results is a medium-security system with some high-level characteristics. Depending on its capabilities, a high-level system could achieve maximum security by the addition of a neutralizing capability. By using modern methods, materials, and technology, a maximum-security system can be developed or an existing system upgraded.

This chapter focuses on several examples of components that could result in maximum security. When the term *maximum security* is used, it denotes the high level of physical security offered by the total system. There is little discussion of less than high-security components, such as wooden doors, local alarm systems, and simple fences, because their presence in a maximum-security environment is incidental and does not significantly contribute to the maximum-security concept.

Maximum security is security in-depth—a system designed with sufficient diversity and redundancy to allow the strength of one particular component to offset the weakness of another. There is no set rule regarding the number of protective layers; again, it depends on the material being protected. As a general rule, however, the more layers, the more difficult it is to defeat the total system. For years the Nuclear Regulatory Commission has inspected nuclear facilities on a component-specific basis. Such an evaluation certainly can point out weaknesses in any component, but by no means does it attest to the effectiveness of the total system. Maximum security depends on the total system, not on its individual components.

The Psychology of Maximum Security. The concept of maximum security is as much psychological as it is physical. To the casual criminal, a maximum-security facility is a target to be given up in favor of a minimum- (or zero) security facility. To the security director, maximum security accurately describes the system of protection designed to allow him or her to go home at night with the conviction, real or imagined, that the assets entrusted for protection will still be there in the morning. To the average citizen, maximum security is a state of mind more than physical components.

When designing a protection system, one can capitalize on the psychological aspects of maximum security. If a system can create the appearance of impenetrability, then it has succeeded in deterring some lesser adversaries. The same principle can be seen when one compares a threat dog to an attack dog. The former has been trained to put on a show of aggression, while the latter has been trained to carry out the threat—a case of bite being worse than bark.

While the concept of maximum security may deter those not up to the challenge, it will not turn aside those who are. Whenever the value of the protected assets exceeds the degree of perceived risk, there will always be takers. For a criminal to act and, for that matter, a crime to be committed, there must be desire and opportunity; the criminal must want to commit the act and must have the opportunity. The effectiveness of the system can be measured in terms of eliminating the opportunity, and the psychology of the system can be measured in terms of eliminating the desire.

The desire to commit a crime can be eliminated or reduced in a variety of ways. The result is that the criminal feels the risk outweighs the treasure and moves on to another target. The strongest reason for a criminal to lose desire is the threat of getting caught. The possibility of apprehending the criminal may be increased by the use of lighting for observation capabilities, barriers that delay intrusion, alarms that signal an intrusion, and a security force that can neutralize intrusion. For the maximum psychological effect to be achieved, the capabilities of the protection system must be known to the criminal, that is, they must convince the criminal that the odds of getting caught are high. This can be accomplished by posting signs in and around the facility advertising its protection. The capabilities of the system should be announced, but details should be considered proprietary information and safeguarded accordingly. This is the primary reason that certain details of maximum security (e.g., radio codes, access controls, locks) are changed whenever key personnel terminate their employment. It is far simpler and cheaper to attempt to eliminate a criminal's desire than it is to eliminate the opportunity.

There are those who disagree on the value of advertising a security system's capabilities. They feel that maintaining a low profile somehow contributes to the overall effectiveness of the system and that criminals will not know that an attractive target exists. This philosophy can be called the *ostrich syndrome*; it may have been true before the advent of mass media and multimedia, but it certainly is not today. A security director who plans to maintain so low a profile that a criminal will be fooled is merely risking the assets he has been entrusted to protect. Rather, anyone scrutinizing a protected facility, passively or actively, will understand that he or she will have to plan carefully and more than likely enlist additional help.

It is important, therefore, that consideration be given to the psychological aspects of maximum security when designing or maintaining a system. An implied presence can do wonders in dissuading criminals from targeting a facility.

THE VALUE OF PLANNING

When setting up a maximum-security system, the best results come from a careful and detailed plan. Two basic questions must first be answered:

1. What is being protected? What assets?
2. How important is it? (This is measured in terms of political and economic impact, corporate commitment to its protection, and health and safety of the public.)

A third question is sometimes asked: Do the costs of protecting it outweigh its value? This may be a consideration when planning for a security system less than maximum, but it is tacitly implied that something calling for maximum security is worth the cost to someone. Once these questions have been answered, planning can commence.

One of the best approaches to take is to list the basic prerequisites of the security system. As was previously stated, maximum security is designed to impede, detect, assess, and neutralize all unauthorized external and internal activity. Under each prerequisite are listed those components that would accomplish these tasks. If the system includes a capability to neutralize, this is stated and provided for accordingly:

- Security force
- Response force
- Coordination with local law enforcement authorities (LLEA)

Next, decide which components are going to be used to impede (Table 4-1), detect (Table 4-2), assess (Table 4-3), and (if necessary) neutralize (Table 4-4).

Once it is decided which components will be used to make up the maximum-security system, attention should be directed to developing a design-reference threat.

TABLE 4-1 Components to Impede

Physical Barriers	Locks
Perimeter fence	Perimeter fence
High-security doors	Openings
High-security windows	Designated doors
Vault	
Security Force	**Access Controls**
Manning levels	Protected areas
Training	Vital areas
	Equipment

TABLE 4-2 Components to Detect

Alarm Systems
Doors
Perimeter
Protected areas
Vital areas

TABLE 4-3 Components to Assess

Lighting	Communications	CCTV
Perimeter	On-site	Perimeter
Protected areas	Off-site	Protected areas
Vital areas		Vital areas

TABLE 4-4 Components to Neutralize

Security Force	Response Force	LLEA Coordination
Manning levels	Manning levels	Contingency planning
Training	Training	Training drills
Equipment	Equipment	

Design-Reference Threat

The design-reference threat defines the level of threat with which the facility's physical protection system could contend (or is designed to defeat). This is a most important consideration when designing or upgrading a system and is essential for cost-effective planning.

The security director should list all possible threats to a particular facility. For example, a hospital's security director might list the following as conditions or situations the system should be able to defeat:

- Emergency room coverage
- Pharmacy coverage
- Disorderly conduct
- Internal theft or diversion
- Assaults on employees or visitors inside and outside
- Armed attack on facility
- Burglary
- Robbery, theft of drugs
- Kidnapping, rape
- Auto theft from parking lot
- Hostage incident
- Infant kidnapping
- Biohazardous and radiological waste
- Power loss
- Violent storms

The next step is to evaluate these threats in descending order of credibility, that is, which threats are the most credible based on past experience, loss rates, crime statistics, and so on. The hospital in this example could list, going from the most credible to the least, the following:

1. Internal theft or diversion
2. Auto theft from parking lot
3. Disorderly conduct
4. Assaults on employees or visitors
5. Burglary
6. Robbery
7. Hostage incident
8. Kidnapping
9. Armed attack

In this example, internal theft or diversion is considered a very real possibility (probably based on past experience) followed by theft of automobiles from the hospital's parking lot. Although possible, the threat of armed attack carries low credibility; therefore, it is of far less concern when deciding on the design of and money to be invested in the security system. Once the credible, realistic threats have

been identified and given higher priority, this information can be used to arrive at the design-reference threat.

The types of adversaries that would likely encounter the security system is another area of consideration when determining the design-reference threat. The Nuclear Regulatory Commission describes six generic categories of adversaries as follows:

1. Terrorist groups
2. Organized sophisticated criminal groups
3. Extremist protest groups
4. Disoriented persons (psychotic, neurotic)
5. Disgruntled employees
6. Miscellaneous criminals

The security director should now assess these potential adversary groups in terms of likelihood of encounter, from most likely to least. The hospital's list would probably look like this:

1. Miscellaneous criminals
2. Disgruntled employees and workplace violence
3. Disoriented persons
4. Organized sophisticated criminal groups
5. Extremist protest groups
6. Terrorist groups

The most likely threat group would include petty thieves from within the hospital's workforce.

Time, location, and circumstance influence the likelihood of a threat from a particular group. For example, labor disputes could lead to threats by disgruntled employees; hospitalizing an unpopular political figure could lead to threats by terrorists. In any case, extraordinary circumstances should not influence the determination of likely adversaries but should be considered during contingency planning.

Once the likely threats and adversaries have been determined, it becomes necessary to correlate the two and establish a specific design-reference threat. The process begins by comparing the most credible threats with the most likely adversaries for a particular facility (in this case, the hospital).

1. Internal theft or diversion
   - Miscellaneous criminals
   - Disgruntled employees
   - Organized sophisticated criminals
2. Auto theft
   - Miscellaneous criminals
   - Organized sophisticated criminals
3. Disorderly conduct
   - Disoriented persons
   - Miscellaneous criminals
4. Assaults
   - Miscellaneous criminals
   - Disoriented persons
   - Organized sophisticated criminals
5. Burglary
   - Organized sophisticated criminals
   - Miscellaneous criminals
6. Robbery
   - Disoriented persons
   - Miscellaneous criminals
7. Hostage incidents
   - Disoriented persons
   - Miscellaneous criminals
   - Disgruntled employees
   - Extremist protesters
8. Kidnapping
   - Organized sophisticated criminals
   - Terrorists
   - Extremist protesters
   - Miscellaneous criminals
9. Armed attack
   - Terrorists
   - Extremist protesters

There is always overlap among adversary groups, and this fact must be kept in mind when preparing a threat-versus-adversary analysis. In the example here, the hospital's security director has defined the primary threat to the facility as internal theft or diversion and the most likely adversaries in this area as miscellaneous criminals followed by disgruntled employees and organized sophisticated criminals. The protection system must be designed or upgraded to counter the most real threat. The most worthy adversary, however, appears to be an organized sophisticated criminal, probably because of the hospital's

drug supply. Although the least likely adversary in this threat, this is the most capable (in terms of desire, resources, and capability); therefore, the system must be designed to defeat him or her. At the same time, adversaries of lesser capability will also be defeated. A very simple analogy illustrates this principle: A screened door, if properly installed, keeps out flies; it also keeps out wasps, butterflies, and birds.

Continuing the process of determining the adversary most capable of carrying out the most credible threats, the hospital's security director probably comes up with the following results:

1. Internal theft—organized sophisticated criminals
2. Auto theft—organized sophisticated criminals
3. Disorderly conduct—disoriented persons
4. Assaults—organized sophisticated criminals
5. Burglary—organized sophisticated criminals
6. Robbery—miscellaneous criminals
7. Hostage incident—terrorists
8. Kidnapping—terrorists
9. Armed attack—terrorists

Planning a system to address a realistic security concern as well as the adversary most capable of causing that concern allows the system's architect to prepare for the worst possible case and least capable adversary alike.

Establishing the design-reference threat, therefore, is contingent on determining the groups to which the specific threats or adversaries belong:

- Internal theft (crimes against property)
  - Auto
  - Burglary
- Violent conduct (crimes against persons)
  - Robbery
  - Disorderly conduct
  - Assaults
  - Hostage incidents
  - Kidnapping
  - Armed attack

On this basis, the hospital's security director knows where to channel resources and the degree of protection needed. Since internal theft or diversion has been defined as the most credible threat, the system should be designed to counter this crime as it would be perpetrated by an organized sophisticated criminal. This is where a great deal of budget money is used. The next most credible threat is auto theft from the parking lot. Again, resources have to be directed to counter auto theft perpetrated by an organized sophisticated criminal. At the other end of the scale, an armed attack on the facility is a very remote possibility. If it were to happen, chances are the act would be perpetrated by terrorists. Since the possibility is quite low, attention and resources (and budget money) are minimal if any in this area, and they more than likely consist of contingency planning or local law enforcement coordination.

The design-reference threat and its supporting analysis become the basis for planning the measures to be instituted to preclude its occurrence or counter its effects.

Example 4-1 A Nuclear Fuel Cycle Facility

Determining the design-reference threat for a nuclear fuel cycle facility, for example, would follow the same process.

1. Possible threats
   - Internal theft or diversion
   - Armed attack
   - Hostage incident
   - Burglary
   - Civil disturbance
   - Auto theft
   - Sabotage
   - Employee pilferage
   - Kidnapping
   - Robbery
   - Assaults
2. Credible threats (most to least)
   - Internal theft or diversion of nuclear material
   - Sabotage (including threats)
   - Armed attack (as a prelude to other action)
   - Civil disturbance (including antinuclear demonstrations)
   - Employee pilferage (of non-nuclear material)
   - Assaults
   - Auto theft (from parking lot)

- Kidnapping
- Hostage incident
- Burglary
- Robbery

3. Potential adversaries (most to least)
   - Terrorist groups
   - Disoriented persons
   - Disgruntled employees
   - Extremists or protesters
   - Miscellaneous criminals
   - Organized sophisticated criminals
4. Match-up of threats and adversaries
   a. Internal theft or diversion
      - Disgruntled employees
      - Disoriented persons
      - Terrorists

   b. Sabotage
      - Terrorists
      - Disoriented persons
      - Disgruntled employees

   c. Armed attack
      - Terrorists

   d. Civil disturbance
      - Extremists or protesters

   e. Pilferage
      - Miscellaneous criminals

   f. Assaults
      - Disoriented persons

   g. Auto theft
      - Miscellaneous criminals

   h. Kidnapping
      - Terrorists
      - Disoriented persons

   i. Hostage incident
      - Terrorists
      - Disoriented persons
      - Disgruntled employees

   j. Burglary
      - Miscellaneous criminals

   k. Robbery
      - Miscellaneous criminals

   l. Most credible threat—most capable adversary
      a. Internal theft or diversion—terrorists
      b. Sabotage—terrorists
      c. Armed attack—terrorists
      d. Civil disturbance—extremists or protesters
      e. Pilferage—disgruntled employees
      f. Assault—disoriented persons
      g. Auto theft—miscellaneous criminals
      h. Kidnapping—terrorists
      i. Hostage incident—terrorists
      j. Burglary—miscellaneous criminals
      k. Robbery—miscellaneous criminals
   - Basic generic threats
      a. Theft
         - Internal and external
         - Pilferage
         - Auto
         - Burglary

      b. Violence
         - Sabotage
         - Armed attack
         - Civil disturbance
         - Assault
         - Kidnapping
         - Hostage incident
         - Robbery

We can see that a nuclear fuel cycle facility's prime security concern is the theft or diversion of nuclear material. The most capable adversary (although the least likely) is a terrorist group. Although theft may be the most serious concern, other violent actions, including sabotage and armed attack, are very real possibilities. The chance of a fuel cycle facility being burglarized or robbed (in the traditional sense) is negligible due to the heavy protection provided. The security director must therefore base this system on a design-reference threat that reflects the most serious concerns. The Code of Federal Regulations requires that nuclear fuel cycle facilities "must establish and maintain…a physical protection system…designed to protect against…theft or diversion of strategic special nuclear material and radiological sabotage." The Code describes the threats the system must be able to defeat:

1. Radiological or biological sabotage. (i) A determined violent external assault, attack by stealth, or deceptive actions, of several persons with the following attributes, assistance, and equipment: (A) well trained, (B) inside assistance, which may include a knowledgeable individual who attempts to participate in a passive role, an active role, or both, (C) suitable weapons, up to and including hand-held automatic weapons, equipped with

silencers and having effective long-range accuracy, (D) hand-carried equipment, including incapacitating agents and explosives; (ii) an internal threat of an insider, including an employee (in any position).

2. Theft or diversion of formula quantities of strategic special nuclear material. (i) A determined, violent, external assault, attack by stealth, or deceptive actions by a small group with the following attributes, assistance, and equipment: (A) well trained, (B) inside assistance, which may include a knowledgeable individual who attempts to participate in a passive role, an active role, or both, (C) suitable weapons, up to and including hand-held automatic weapons, equipped with silencers and having effective long-range accuracy, (D) hand-carried equipment, including incapacitating agents and explosives, (E) the ability to operate as two or more teams; (ii) an individual, including an employee (in any position); and (iii) conspiracy between individuals in any position.

In summary, a design-reference threat is a systematic analysis of all possible threats and adversaries so that credible threats and adversaries can be identified and this information used as a basis for planning and implementing a physical protection system.

Layering for Protection

The designer must remember the principle of security in depth. Protection must be layered to provide diversity and redundancy (Figure 4-2). Whenever and wherever possible, layer components. Conduct a walk-through of the facility and likely threat routes. Start either at a point outside and work in, or start at the most sensitive point within the facility and work out.

PHYSICAL BARRIERS

Physical barriers should be checked at the area considered the most sensitive, such as the vault, cell block, tool crib, or shipping department. This area is called the objective.

1. Provide a high-security barrier around the objective.

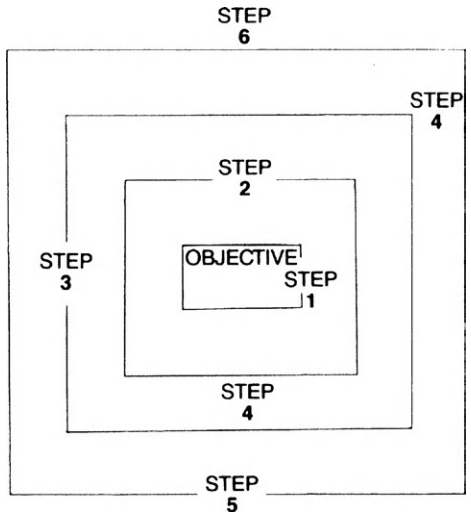


FIGURE 4-2 Layering. *(Reprinted with permission from* Security Management*.)*

2. Enclose a high-security barrier within another high-security barrier.
3. Surround the outer barrier with a penetration-resistant fence.
4. Establish isolation zones on either side of the penetration-resistant fence.
5. Surround the outer isolation zone with yet another penetration-resistant fence and isolation zone.
6. Establish an isolation zone on the outside of the outermost fence.

Entry and exit points should be identified and those vital to the effectiveness of the total system determined. High-security doors and windows must be installed or upgraded where appropriate. As a general rule, if a window is not needed at a particular location, it should be eliminated. The area containing the objective should be a vault or other such strong room, depending on cost considerations and the effectiveness of the total system. It is important to evaluate the structural components of the facility, including walls, ceilings, and floors, and determine their ability to withstand a threat equivalent to the design-reference threat.

Physical barriers are not exclusively for keeping someone out. They can also be used to keep someone in.

Locks

After deciding which openings require locks (high-security and otherwise), the types of locks are selected. The use of a single Grand Master combination for any mechanical locking system is not considered a sound security practice.

Access Controls

Protected and vital areas are designated and a decision made as to who will be admitted to the facility and who will be allowed unrestricted access within it. Generally, the protected area includes the facility and the outside area around it, up to the first penetration-resistant fence. Vital areas include the vault or strong room and could include the alarm stations, emergency generator buildings, or other areas that could be considered vital to the protection of the objective and the facility. (One must not overlook the possibility that the facility, rather than its contents, could be the target of an action.)

Security Force

Appropriate staffing levels of the security force for each shift are established, with the amount of training necessary and desirable. (Some states have mandated training levels for security officers.) The force is equipped with resources to handle the design-reference threat.

Alarm Systems

A maximum-security system should have a state-of-the-art perimeter alarm system capable of detecting an intrusion anywhere on the perimeter. Additionally, all vital areas should be equipped with alarms capable of detecting the presence of an intruder. All doors that contribute to the protection system should have alarms that are continuously monitored by a person in a remote location on-site. Alarm circuits should be supervised so that tampering with the system or its components causes an alarm.

Lighting

The value of lighting should be considered for impeding as well as for assessing. In deciding where security lighting should be directed, it should be kept in mind that proper placement avoids silhouetting security personnel. High-intensity glare lighting, positioned to illuminate the isolation zone outside of the protected area, is always appropriate in a maximum-security environment. Also, inside areas can be illuminated to facilitate the use of state-of-the-art CCTV, thus saving money on expensive low-light cameras, energy costs notwithstanding.

Communications

The ability to communicate on-site is of vital importance to the security force. Consider the alternatives for communications. In addition to commercial telephones, the security force should be equipped with at least one dedicated and supervised hotline to LLEAs and a two-way radio network. Each officer should have a two-way radio and the system should have at least a two-channel capability. Additionally, the facility should be able to communicate with the LLEA by two-way radio.

CCTV

The CCTV cameras should be placed to ensure proper surveillance and assessment. Depending on the type and quality of equipment, the perimeter and protected and vital areas can be effectively monitored.

Response Force

If the nature of the security system requires it to neutralize a threat, attention must be directed toward establishing a response force of security personnel properly trained and equipped for that purpose. The number of personnel constituting a response force should be sufficient to counter the design-reference threat.

LLEA Coordination

When a system has been designed or upgraded to safeguard something that requires protection of this magnitude, local law enforcement authorities should be brought into the picture. It always helps to establish a liaison very early in the game. Once the cooperation of LLEA is secured, it is helpful to consult with them on contingency planning to meet the design-reference threat and, if possible, schedule joint training sessions and drills to exercise the plans.

Once the process of analysis has been completed, it is time to plan the security system. It is much easier to incorporate security features when a facility is constructed. In this respect, corporate support is essential. The security director should work with the architects and contractors throughout the construction. When this is not possible and an upgrade to an existing facility is necessary, the security director more often than not becomes the chief architect of the upgrade. Whenever this happens, the value of planning as discussed becomes evident, as it is the basis for the formal security setup.

THE SECURITY PLAN

The security plan is frequently contracted out to a consultant who works with the security director. Before system implementation, it is a necessary building document; after implementation, it becomes a necessary reference document. Needless to say, the plan should be treated as proprietary, and access to it should be restricted to those who have a *need to know*.

The plan can take many forms and contain a great deal of information. In its basic sense, it is a description of the protection system and its components. Detail can be as much or as little as desired by the security director. For use as a building document, however, it should be quite detailed. Information can be deleted after implementation, but if the facility is regulated by an agency that requires safeguards, the plan may require many details. If this is the case, the document should be treated as sensitive.

The security plan should contain, but not necessarily be limited to, the following information:

1. A description of the facility and its organizational structure.
2. The security organization of the facility.
3. A discussion of the physical barriers used in the system.
4. A discussion of the alarm system used.
5. A description of access controls used to restrict access to or within the facility.
6. A discussion of security lighting at the facility.
7. A description of the communications capability.
8. A description of the CCTV capability and its use.
9. A breakdown of the security force, its organization, training, equipment, capabilities, resources, and procedures.
10. A discussion of outside resources including LLEA and others as appropriate.
11. Annual assessments.

Depending on the nature of the facility and its commitment to regulatory agencies, or if the security director so desires, other plans can be developed, such as contingency, training, and qualifications plans.

Justification

When it finally comes down to selling a security design or upgrade to the people who have to pay for it, the job can be made somewhat easier by following a few basic principles.

Most security directors have heard that, "Security contributes nothing to production, is an overhead item, and is a necessary evil." Dealing with the "necessary evil syndrome" has been the subject of much discussion since the business of assets protection started. Good security holds losses to a minimum and keeps down costs, resulting in increased profits. Fulfillment of the security mission can be called negative profit, compared with the positive profit generated by production. Accordingly, security management personnel must justify many, if not all, systems,

expenditures, programs, personnel, approaches, and, at times, their own existence.

Most facilities cut costs for security before anything else; therefore, a planned, systematic approach is necessary to keep this practice to a minimum and secure the resources necessary for efficient security operation. Justification should be based on the following steps:

1. Convincing oneself that a proposal is justified
2. Convincing others it is justified
3. Formulating the approach
4. Presenting the approach

Convincing Oneself That a Proposal Is Justified. It has been said that a good salesperson believes in the product. So, too, must the security director believe in the proposal. Before it can be justified to anyone, it has to be justified in his or her mind. In some cases, this takes only a few minutes and consists of a mental evaluation of the issue. In others, it is a lengthy, detailed examination of alternatives.

As a first step, it is necessary to define the issue—just what is wanted: personnel, equipment, policy, and so on. Then, consider the pros and cons: Do the results justify the expense? Is there a cheaper way to accomplish the same thing? Is it really necessary, and what happens if it is not done? Is there enough money available to finance it?

Next, consider the benefit to the company: Will this increase profits? Not likely. Will this reduce overhead? Possibly. Will this make the job easier? Probably.

Turnaround time must be considered, that is, the time it will take to gain a return or realize a benefit from the expenditure or approach.

The security director must rely somewhat on gut feeling. If it is felt that the proposal is logical and rational but there is a negative gut feeling, set the proposal aside and reconsider it at a later date. Circumstances could change and the whole proposal could become moot.

Convincing Others It Is Justified. Once the proposal is sound, it has to be sold to others, who may see everything involving security printed in red ink. Generally, any money that can be saved, no matter what the percentage, is a plus when justifying a proposal. Money saved is negative profit and should be sold as such.

Before an attempt is made to convince others of the soundness of an approach, the security director must research the whole issue, investing the time and effort proportional to the expense and importance of the issue. Research is based on the company's past experience, personal experience, supporting documentation, and others' perceptions.

Company's Experience. The company may have encountered problems in this area in the past and therefore could be receptive to the idea. An existent policy could support the proposal or eliminate it from the start.

The security director should consider any adverse publicity that could result from implementation of, or failure to implement, the approach. Tarnished company image is perhaps one of the most overlooked areas of corporate concern. If a company is in the midst of a problem that threatens its image, its executives and public relations officers often go to great lengths to preserve its image; however, the inclination to spend money to counter bad press diminishes as time goes by. The tendency to prevent recurrence of an unfavorable situation diminishes as more time elapses. An idea is best promoted hard on the heels of a situation it would have prevented.

Personal Experience. A security director has probably dealt with the same issue before or is familiar with others' handling of a similar issue. Draw on previous experience to define and analyze possible short- and long-term ramifications and positive and negative results.

It is advisable to pay particular attention to idiosyncrasies that could provide necessary direction to the approach and, if possible, capitalize on them. For example, if the approving authority has a liking for gadgets and the approach calls for the use of gadgetry, this affinity could be parlayed into a successful acquisition.

Formulating the Approach

Armed with the raw data accumulated up to this point, it is necessary to adopt a strategy for communicating arguments in a convincing manner.

Formulation of the approach is based on personal knowledge of and experience with the approving authority. If charts and transparencies are generally well received, they should be used; however, the amount of time spent should be in proportion to the magnitude of the project.

If personal experience shows that a concise approach is best, the security director should formulate accordingly. Decide on the format, written or verbal, and prepare for both. Consistency is important; the odds increase in favor of subsequent approvals if credibility has been established. Make a list of areas to be covered by priority (Figure 4-3). Certain basic information must be communicated regardless of the format:

1. Definition of the problem
2. Ramifications
3. Alternatives
4. Elimination of each alternative (except the one proposed)
5. The solution
6. Support for the solution

Presenting the Approach

Once the issue has been researched and an approach formulated, it must be presented. (It is always a good idea to send a memo regarding the issue beforehand.) If a formal presentation is required, it is recommended that the presentation be tested on affected individuals who should be encouraged to offer their critiques.

The first consideration in this report should be timing. Once the presentation commences, the approach should be presented as formulated and include the basic information already discussed. The security director must be concise and consistent, anticipate any questions, and be prepared to answer them. Depending on time and importance, audiovisual aids can be effective, as can handouts; it may be no more than a single-page outline, but it helps to leave something for later reference. Above all, do not oversell.

If, after this effort, the proposal is not approved and you wish to protect yourself, do so with memos to file and other such correspondence, so that if problems result from the proposal's disapproval, it can be shown that you tried.

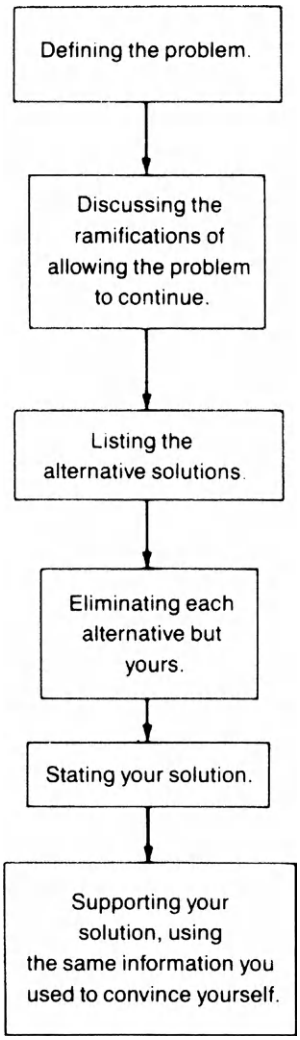

Defining the problem.
Discussing the ramifications of allowing the problem to continue.
Listing the alternative solutions.
Eliminating each alternative but yours.
Stating your solution.
Supporting your solution, using the same information you used to convince yourself.

FIGURE 4-3 The justification process. *(Reprinted with permission from* Security Management*, pp. 30–34.)*

SUMMARY

This chapter was updated and reviewed in 2011. The theory and concepts laid out apply generically across the board. The approaches to physical security are based on the physical protection required to meet the need. Through the use of the risk equation, various proposed upgrades in physical protection at a facility can be compared.

The options that give the best cost/benefit to the facility can be implemented. The risk is normalized to the consequence of loss of the asset and thus the allocation of scarce physical protection resources is appropriately applied to keep all risks at an acceptable level.

REFERENCES

[1] Gigliotti RJ, Jason RC, Cogan NJ. What is your level of physical security? Security Management 1980:46–50.
[2] U.S. Nuclear Regulatory Commission. Generic adversary characteristics summary report. Washington, DC: The Commission; 1979.
[3] United States Code of Federal Regulation, title 10, part 73.1; 1982.
[4] Gigliotti RJ. The fine art of justification. Security Management 1980:30–4.
[5] Garcia ML. The design and evaluation of physical protection of systems. Boston: Butterworth-Heinemann; 2001.

CHAPTER

5

Protective Barriers

Lawrence J. Fennelly, CPO, CSS, HLS III

Protective barriers are used to define the physical limits of an installation, activity, or area. Barriers restrict, channel, or impede access and are fully integrated to form a continuous obstacle around the installation. They are designed to deter the worst-case threat. The barriers should be focused on providing assets with an acceptable level of protection against a threat.

OVERVIEW

Protective barriers form the perimeter of controlled, limited, and exclusion areas. Utility areas (such as water sources, transformer banks, commercial power and fuel connections, heating and power plants, or air conditioning units) may require these barriers for safety standards. Protective barriers consist of two major categories: natural and structural.

- Natural protective barriers are mountains and deserts, cliffs and ditches, water obstacles, or other terrain features that are difficult to traverse.
- Structural protective barriers are humanmade devices (such as fences, walls, floors, roofs, grills, bars, roadblocks, signs, or other construction) used to restrict, channel, or impede access.

Barriers offer important benefits to a physical-security posture. They create a psychological deterrent for anyone thinking of unauthorized entry. They may delay or even prevent passage through them. This is especially true of barriers against forced entry and vehicles. Barriers have a direct impact on the number of security posts needed and on the frequency of use for each post.

Barriers cannot be designed for all situations. Considerations for protective structural barriers include the following:

- Weighing the cost of completely enclosing large tracts of land with significant structural barriers against the threat and the cost of alternate security precautions (such as patrols, WMD teams, ground sensors, electronic surveillance, and airborne sensors).
- Sizing a restricted area based on the degree of compartmentalization required and the area's complexity.

As a rule, size should be kept to a minimum consistent with operational efficiency. A restricted area's size may be driven by the likelihood of an aggressor's use of certain tactics. For example, protecting assets from a vehicle bomb often calls for a substantial explosives standoff distance. In these cases, mitigating the vehicle bomb would often be more important than minimizing the restricted area to the extent necessary for operational efficiency.

Protective barriers should be established for the following:

- Controlling vehicular and pedestrian traffic flow
- Providing entry control points where ID can be checked
- Precluding visual compromise by unauthorized individuals
- Delaying forced entry
- Protecting individual assets

If a secured area requires a limited or exclusion area on a temporary or infrequent basis, it may not be possible to use physical structural barriers. A temporary limited or exclusion area may be established where the lack of proper physical barriers is compensated for by additional security posts, patrols, and other security measures during the period of restriction. Temporary barriers (including temporary fences, coiled concertina wire, and vehicles) may be used. Barriers are not the only restrictive element, and they may not always be necessary. They may not be ideal when working with limited or exclusion areas or when integrated with other controls.

Because barriers can be compromised through breaching (cutting a hole through a fence) or by nature (berms eroded by the wind and rain), they should be inspected and maintained at least weekly. Security-force personnel should look for deliberate breaches, holes in and under barriers, sand dunes building up against barriers, and the proper functioning of locks.

PERIMETER ENTRANCES

Active perimeter entrances should be designated so that security forces maintain full control without an unnecessary delay in traffic. This is accomplished by having sufficient entrances to accommodate the peak flow of pedestrian and vehicular traffic and having adequate lighting for rapid and efficient inspection. When gates are not operational during nonduty hours, they should be securely locked, illuminated during hours of darkness, and inspected periodically by a roving patrol. Additionally, warning signs should be used to warn drivers when gates are closed. Doors and windows on buildings that form a part of the perimeter should be locked, lighted, and inspected.

Entry-Control Stations

Entry-control stations should be provided at main perimeter entrances where security personnel are present. Considerations for construction and use should be based on the information outlined in USACE STD 872-50-01.

Entry-control stations should be located as close as practical to the perimeter entrance to permit personnel inside the station to maintain constant surveillance over the entrance and its approaches. Additional considerations at entry-control stations include:

- Establishing a holding area for unauthorized vehicles or those to be inspected further. A turnaround area should be provided to keep from impeding other traffic.
- Establishing control measures such as displaying a decal on the window or having a specially marked vehicle.

Entry-control stations that are manned 24 hours each day should have interior and exterior lighting, interior heating (where appropriate), and a sufficient glassed area to afford adequate observation for personnel inside. Where appropriate, entry-control stations should be designed for optimum personnel ID and movement control. Each station should also include a telephone, a radio, and badge racks (if required).

Signs should be erected to assist in controlling authorized entry, to deter unauthorized entry, and to preclude accidental entry. Signs should be plainly displayed and be legible from any approach to the perimeter from a reasonable distance. The size and coloring of a sign, its letters, and the interval of posting must be appropriate to each situation.

Entry-control stations should be hardened against attacks according to the type of threat. The methods of hardening may include:

- Reinforced concrete or masonry
- Steel plating
- Bullet-resistant glass

- Sandbags, two layers in depth
- Commercially fabricated, bullet-resistant building components or assemblies

Internal Barriers

Have you ever watched a trespasser come into a building? He walks slowly, he looks around, and his eyes go right and left. He is 8 feet into your lobby and sees the turnstile and realizes he has been denied access. So he proceeds to the security desk with a simple question of employment.

Barriers are psychological deterrents allowing unauthorized access. Turnstiles and access control are physical barriers that control entry points and complement your security program and your security officers.

Functions of structural and/or natural barriers include:

1. *Define* protection area boundaries.
2. *Delay*—slow traffic or access. Consider speed bumps.
3. *Direct* access to garages, parking lots, and building entrances.
4. *Deny* unauthorized access and allow only authorized visitors.

Designing Security and Layout of Site. Designing security into a new or renovated complex can begin with the exterior or interior. Since we are discussing protective barriers in this chapter, let us assume we started the layout discussion on the outside.

Your main lines of defense are your perimeter barriers or the outer edge to your property line. The second line of defense is the exterior of the building, which includes the roof and roof access and walls, doors, and windows. Remember to eliminate all but essential doors and windows. If this is not done in early stages, they will have to be alarmed and set up as emerging exits. Also included should be adequate lighting (cost-effective) that meets standard and supports exterior closed-circuit TV (CCTV). The third line of defense is the interior. It is important to reduce access points by using access control and have specific areas zoned for access control and added security.

Passive Structural Barriers

- Jersey barriers
- Large boulders or rocks
- Large round cement stones
- Roadblocks or closed roads
- Fences
- Gates
- Bollards at entrances

Active Structural Barriers

- Hydraulic bollards
- Motor-operated lift-arm gates
- Pop-up wedges
- All geared to control traffic for entrances and exits

BARRIER PLANNING

When planning a perimeter barrier, the following should be taken into account:

- Walls are usually more expensive than fences, observation enclosures, CCTV, and exterior lighting. Opaque fences may provide a cheaper alternative.
- Fences and walls provide only limited delay against intruders; the least secure types can only delay a skilled intruder for a few seconds. A perimeter barrier intended to provide substantial protection against intruders should therefore combine a fence or wall with security lighting, an intruder detection system, CCTV, and security guard forces.
- The perimeter should be as short as possible and illuminated.
- The perimeter should run in straight lines between corner posts to facilitate surveillance.
- Drains or culverts giving access beneath the perimeter barrier should be protected.
- The ground on both sides of the perimeter barrier should be cleared to deny cover to an intruder.

- Emergency gates may be required to provide safe evacuation routes.
- A sterile zone protected by a double fence may be required for certain types of intruder detection sensors.
- A security guard force should support the perimeter security system.
- Exterior emergency phones should be connected to the security officer's desk.
- Barriers are deterrents. They come in a variety of acceptable sizes and shapes.

FENCE STANDARDS

The perimeter should have a fence or wall that meets the requirements of local planning and licensing authorities while remaining an effective deterrent against intruders. As a guide, any fence less than 7 feet high is unlikely to do more than demarcate a boundary.

Generally, the basic perimeter fence should have concrete fence posts with three strands of barbwire at the top. The barbwire should be at a 45-degree angle pointing upward and outward. The foot-tall chain-link fences should be embedded in a concrete curb in the ground that slants away on both sides from the fence to shed water and be buried deep enough to prevent burrowing.

Where local factors require an enhanced level of security, anti-intruder fencing is recommended to a height of 7 feet with razor or barbwire at the top. The base of the fence should be embedded as previously described.

Where the value of the protected side is particularly high and there is known risk (such as terrorist attack), consideration should be given to augmenting the selected fence with security lighting, CCTV, an intruder detection system, and a security guard force.

TYPES OF SECURITY FENCES

The following fences are available for security use, and are listed in ascending order of their effectiveness against intrusion:

- Industrial security chain-link fence.
- Standard anti-intruder chain-link fence.
- Standard steel palisade fence, security pattern standard expanded metal (Expamet) security fence.
- High-security steel palisade fence.
- Power fencing. This is similar to cattle fencing in that it will give an electric shock to anything touching it. This type of fencing is generally safe to use around hydrocarbon sites, but the manufacturer's advice should be sought on its exact deployment. Power fencing sends an alarm when touched, thus making it a barrier with intruder detection. It is also good to use above walls in high-risk areas on domestic properties.
- Palisade fences are more expensive than chain-link fences but have better potential upgrading to increase effectiveness against intruders and for the addition of fence-mounted intrusion detection sensors. Galvanized palisade fences have a much longer life than chain-link fences, Expamet, or weld-mesh fences. The high-security fences are significantly more effective against intruders than the other fences.

SUMMARY

Keep in mind that structural barriers physically and psychologically deter and discourage the undetermined, delay the determined, and channel the traffic flow through entrances.

REFERENCES

[1] FM 3-19.30, Field Manual Department of Army, Protective Barriers. 1979; Chapter 4, Section 4-1, March 1.
[2] Tyska L, Fennelly F. Physical security—150 things you should know. Boston: Butterworth-Heinemann; 2000.

CHAPTER

6

Physical Barriers*

Richard Gigliotti, Ronald Jason

When we speak of physical barriers, most people tend to think in terms of reinforced concrete walls, chain-link fences topped with barbwire, modern bank vaults, and other such apparent applications of maximum security. We can think back, however, to the Roman Empire, whose power and influence extended over what was then almost all of the known world. The continuance of this power was guaranteed by the establishment of outposts throughout the conquered territories controlled by powerful Roman legions. These outposts were actually fortified garrisons—an example of using physical barriers for protection of a base of operations.

This same principle has been used throughout recorded history: the British and Colonial fortresses during the Revolutionary War, the U.S. Army forts in the Indian territories during the last half of the nineteenth century, the French Maginot Line in World War II, and even the protected base camps established by American forces in Vietnam. It is interesting to note that the last were actually a variation of the system of forts used during the Revolutionary War to which forces could retire with a relative degree of safety for rest and re-equipping.

The concept of physical barriers is not unique to *Homo sapiens*. When a monkey climbs a tree, it takes advantage of a natural barrier in its environment, which provides a form of physical security. While in the tree, it is out of danger from the carnivores that prowl the jungle floor, although not completely safe from attack by other natural enemies.

People have used barriers to enhance physical security throughout history. Our earliest forebears had the instinctive need for physical security in its most primitive form: the cave and the tree. Certainly, the need for some edge in the game of survival was crucial to our continued existence. We could not outrun the saber-toothed tiger and giant wolf, we had no protective shell like that of the giant tortoise, we could not intimidate our enemies by sheer size like the mastodon, and our reproductive capacity was limited. Only by using the security provided by climbing the nearest tree or taking shelter in a handy cave were we allowed the necessary time to continue progress along the evolutionary path.

As intelligence increased over the centuries, we understood that certain changes and improvements could be made to the natural shelter available. There was not much to do to a tree, but by dragging rocks, boulders, and fallen trees across the mouth of his cave, a person could erect rudimentary walls and fences—physical barriers that enhanced the natural protection. The eventual addition of animal skins to cover the openings in cave dwellings was another sign of the march toward civilization and another component in developing physical security.

*Originally from Gigliotti R, Jason R. Security design for maximum protection. Stoneham, MA: Butterworth-Heinemann, 1984. Updated by the editor, 2011.

DOORS

The modern equivalent to the cave dweller's animal skin is the door. The function of a door in physical security is to provide a barrier at a point of entry or exit. The function of a door in maximum security is still to provide such a barrier; however, the barrier must also be impenetrable by ordinary means and offer the maximum delay time before penetration by extraordinary means (i.e., by the use of cutting tools, hand-carried tools, and some explosives).

During construction of a maximum-security facility, it is necessary to define the function of all doors and their relationship to the total protection system. When an existing door is evaluated, the function must again be defined and include the area or material protected.

It is not necessary to make all doors maximum security—only those that are essential to the effective functioning of the total security system. Once a particular door is designated to be incorporated into the overall system, it must be upgraded to provide maximum security. There are two options in this respect: replace the door with a commercially available, penetration-resistant model or upgrade it to provide the necessary resistance. Obvious areas of concern when dealing with maximum-security doors are door hinges and hardware.

Personnel Doors

The average industrial personnel door is a hollow steel composite door with 18-gauge metal facing. It is usually hung on butt hinges with nonremovable pins and may open in either direction. It may have ventilation louvers or glass panels. According to the *Barrier Penetration Database*, the hollow steel door can be penetrated in one minute or less by various methods, including:

1. Defeat of the locking mechanism, if a knob is accessible, by using a half-pound pipe wrench to break it (0.4 ± 0.08 minutes)
2. Prying the door open using a 15-pound pry bar (0.2 ± 0.04 minutes)
3. Penetration using a 10-pound fire axe (3.8 ± 0.08 minutes)

Hollow steel doors can be made more penetration resistant by a variety of methods:

1. Bolting or welding a steel plate to the inside or outside of the door (especially if louvers or glass is present).
2. Installation of several dead bolts that go into all four sides of the door frame.
3. After removing the metal back, welding ¼-inch steel louvers on the inside of the front panel of the door, 3–4 inches apart from top to bottom, and replacing the back door panel (Figure 6-1).
4. Replacing hardware with more penetration-resistant types or upgrading existing hardware.

By upgrading the hollow steel door, additional weight is added and this is a consideration when evaluating hinges and hardware. In most cases, hinges have to be reinforced to compensate for the added weight.

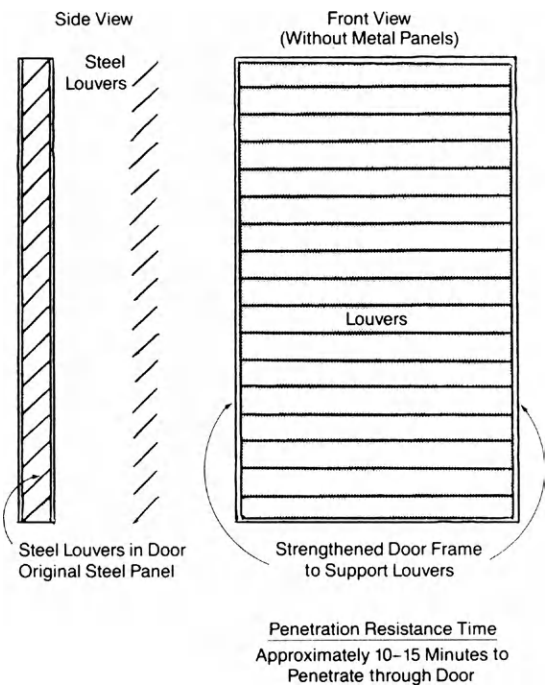


FIGURE 6-1 Hardened door. (Courtesy of U.S. Army Material Systems Analysis Activity.)

Substantial steel doors or security-class doors are commercially available, made of ¾-inch steel on one side and ⅛-inch steel on the other and filled with 3 inches of fiberglass or similar material. Ten pounds of bulk explosives take 1.5 ± 0.3 minutes to penetrate this type of door.

In addition to the door-hardening techniques previously mentioned, ready-made security panels have been marketed under the name DELIGNIT® by Blomberger Holzindustrie of Blomberg, West Germany. This product is constructed from highly tempered plate material consisting mainly of hardwood veneers (primarily beech), cross-laminated, and bonded under pressure with phenolic resins. The material is available in thicknesses of 20, 30, 40, and 50 mm in a variety of standard sizes, as well as in specially ordered sizes and thicknesses, and is suitable for construction of bullet-resistant and burglar-impeding doors, partition walls, and so on.

Tests conducted by official agencies in West Germany and Great Britain indicate successful resistance of a sample 30 mm panel to a limited variety of small arms fire up to and including .357-caliber magnum and 12-gauge shotgun. In addition, a test was conducted in which two 30 mm sections of DELIGNIT® panel spaced 150 mm apart were subjected to fire from a military rifle firing the 7.62 NATO standard round. The result of a series of five shots was that no bullet penetrated the inner of the two panels.

While the manufacturer does not provide a finished door, it can provide the names of door fabricators that have experience with its material. The manufacturer claims that it can be worked by any carpentry shop equipped to handle hardwood veneers, although use of carbide-tipped cutting tools is recommended.

Frames for maximum-security doors should be anchored to the wall in such a manner that penetration resistance is at least equal to that of the door. If at all possible, hinges should be inaccessible from the side of the door that would face the likely threat. As an alternative, individual hinges should be case hardened or replaced with a heavy-duty, case-hardened piano hinge and the hinge pins made unremovable by welding or pinning (Figure 6-2).

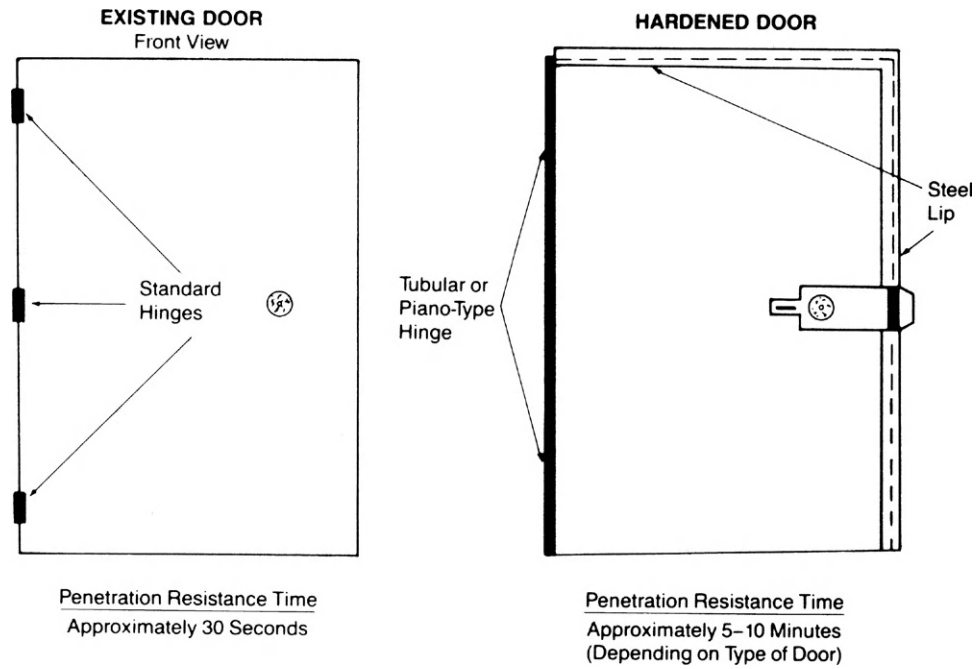


FIGURE 6-2 Hardening door jamb seam, hinges, and locking devices. (Courtesy of U.S. Army Material Systems Analysis Activity.)

Additionally, some consideration should be given to installing ¼-inch steel plates over exposed hinges, which offer an additional barrier to cutting and require somewhat more explosives to defeat. Another way to increase the resistance of hinges is to mortise them into the door jamb and door, thus exposing little if any of the hinge pin. The installation of a piano hinge on the outside of the door and jamb would provide a barrier to the support hinges.

A simple yet effective application of the dead bolt principle previously mentioned is to install ½-inch steel rods, equidistant between support hinges, on the inside of the door. On the inside door jamb, install a ¼-inch steel plate that has been drilled to accept the rod. If the hinges are defeated, the arms continue to hold the door secure.

An existing security-class door can be hardened to increase penetration time from 1–2 minutes to 20–30 minutes by welding heavy angle iron or small structural I-beam to form a 14-inch or smaller grid on the inside of the front door panel (without interfering with the locking mechanism; Figure 6-3).

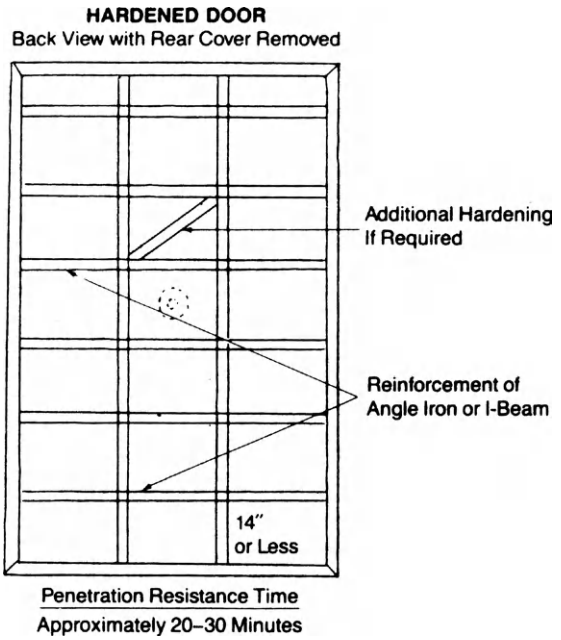


FIGURE 6-3 Hardening fire-class or improving security-class doors. (Courtesy of U.S. Army Material Systems Analysis Activity.)

No high-security door should have its hardware and hinges accessible from the side from which a threat is likely. Doors should open toward the likely threat direction.

In addition to the solid maximum-security doors discussed thus far, several companies make turnstile-type doors. These are useful for controlling access; however, they have no use as high-security barriers.

Retrofit Upgrading of Existing Doors

To harden an existing door against tool attack, the customary practice is to clad the attack side with heavy-gauge sheet metal or steel plate. This solution has as its principal merit the fact that it can be implemented quickly with materials purchased locally. Cladding should be applied only to solid or laminated wood or substantial hollow metal doors. The thinnest recommended cladding material is 12-gauge steel sheet. It must be securely fastened to the door using carriage bolts with the nuts applied from the protected side. The nuts should be tack-welded to the bolts to prevent removal or, alternatively, the ends of the bolts can be peened to serve the same function. Bolts should be no less than $^{5}/_{16}$ inches in diameter and should be spaced from 6 to 10 inches apart and as close to the edge as the door frame allows, preferably no more than 1 or 2 inches.

If the cladding is applied to an outward-opening door, it will probably be necessary to provide protection to the free edge of the cladding to prevent it from being pried up and peeled off the substrate. This can be accomplished by forming the sheet metal cover so that it wraps around the door edges, or it may be practical to build up the outside face of the door frame with a steel guard that denies access to the edge of the cladding.

Experiments were conducted at the Navy Construction Battalion Civil Engineering Laboratory in the use of 9-gauge, low-alloy high-strength steel sheet and ¾-inch plywood to build up a laminated veneer for retrofit hardening. A 2-inch laminated panel consisting of exterior

steel layers, one central steel layer, and two plywood layers (S-P-S-P-S), was found to have the added merit of stopping all calibers of pistol fire and high-powered rifle fire up to and including .30–.06 military ball rounds. A door constructed on this system has the merits of both attack and bullet resistance.

With retrofit cladding, it is necessary to take into account the effects of the door fit due to the additional thickness and the problem of additional weight. To install this heavy door it is necessary to provide for mounting with heavy-duty hinges and protect against hinge-pin removal and hinge destruction if resistance against attack is to be accomplished.

The door recommended for this application is a hollow door with a skin of 12-gauge cold-rolled steel reinforced by internal channel stiffeners of 22-gauge or thicker steel. The hollow spaces between the stiffeners may be filled with suitable material as needed for thermal insulation.

Door Frames

The high-security door system does not present full resistance to attack and penetration unless the frame is hardened to a level similar to that of the door. Similarly, the attack resistance of the frame means little without commensurate strength of its attachment to the surrounding wall and the door. In fact, to be effective, the doors, frames, and wall attachments must be designed as attack-resistant assemblies.

The frame should be fabricated of 16-gauge or thicker steel. To strengthen and support it against being spread apart or crushed by hydraulic jacks or other tools, the frame (jambs and head) must be filled with a suitable cement grouting and bonded to and backed by the wall structure surrounding the door system.

Hinge Vulnerability and Common Countermeasures

Door installations in which the hinges are located on the exterior side of the frames are vulnerable to unauthorized entry through attack on the hinges. It is frequently possible to use a drift punch and hammer to drive out the hinge pin and open the door from the hinge side. Alternatively, the hinge knuckle can be cut off with a hacksaw, cold chisel, or torch and entry made.

The most common countermeasures to that threat are to inhibit or prevent the removal of the hinge pins. This is most frequently done by peening over or tack-welding the ends of the pins. Another approach is to install a set screw in the knuckle so that it locks the pin in place. Peened and welded hinge pins can be freed by filing off their ends and driving them out. Set screws are seldom effective in resisting an attack with a drift pin and hammer. Still another technique is to use a continuously interlocking hinge system running the full length of the door (piano hinge).

Some manufacturers make hinges in which the knuckles completely cover the ends of the hinge pins and thus prevent their being driven out with a drift pin. Regardless of how the pin is protected, if the knuckle is exposed on the outside, it is generally possible to saw off or otherwise remove or destroy the assembly and thus gain entry by prying open the door from the hinge side.

Door and Frame Interlocking

Various countermeasures have been used to prevent entry through destruction or removal of the hinge pin or knuckle assembly. The most common of these is to install a substantial protruding steel dowel pin in the hinge edge of the door or frame and a mating socket or hole in the frame or door so that the pin engages in the socket when the door is closed. In this manner the door and frame are interlocked automatically whenever closed, and removal of the hinge does not allow opening the hinge side. Using this basic approach, one can devise a variety of pin-in-socket, tongue-in-groove, or other similar devices to provide interlocking on the hinge side of the door. In the case of large fabricated steel doors, it is simple to orient the channel-iron framing member (on the hinge side) so that it creates a cavity (groove) into which a corresponding angle iron (tongue), which is welded to the door frame, can engage. In view

of the relatively simple nature of the design and installation of positive interlocking hardware (i.e., internal steel dowel, pin in socket, or tongue in groove) for coupling the hinge sides of the door to the frame, it is recommended that this practice be used wherever highly valuable, critical, or sensitive assets are secured. The following is quoted from the Sandia Laboratories' *Barrier Technology Handbook*.

> *Doors, due to their functional requirements and associated hardware, impose design restrictions and are in many cases, one of the weakest links in a structure. For barrier purposes, the principle of balanced design requires that doors with associated frames, hinges bolts, and locking mechanisms be strengthened to afford the same penetration delay as is provided by the floors, walls, and ceilings of the parent structure. Conversely, if the door structure cannot be enhanced, it may not be cost-effective to upgrade the existing structure. No currently available standard or commercial doors or hardware provide significant resistance against determined adversaries.*

Hinges Appropriate for Door Weight

In designing the hinge system, the weight of the door must be considered. For example, a door designed for resistance against tool attack only might weigh 10–15 pounds per square foot and could be hung on butt hinges, particularly if the door is used infrequently.

Vehicle Doors. The standard security vehicle overhead door found in many facilities is usually of the corrugated steel, roll-up variety. These doors are ordinarily constructed of 16-gauge steel with a stiffness required to withstand 20 pounds per square foot of wind pressure and can be easily penetrated. Using a 6-foot pry bar and a 2 × 4 plank weighing 20–25 pounds, penetration time is 0.8 ± 0.2 minutes. Hardening this type of door is difficult; therefore its use in a maximum-security environment should be kept to a minimum. Specifically designed vehicle doors are usually constructed of at least ¼-inch steel plate and are more penetration resistant. Table 6-1 shows estimated penetration times for standard vehicle doors. Corrugated roll-up and hollow steel panel doors offer little resistance to explosive attack; delay time is governed by the setup, retreat, return, and crawl-through times. Thermal cutting by torch or oxy-lance (burn bar) affords the same delays as for a personnel door. The material thickness of the panel door requires more time than the corrugated door material.

Hand-carried tools, such as jimmy bars and axes, can be used to penetrate a vehicle door. A vehicle may be used to effect penetration quickly when the noise associated with such an attack is not a major consideration. Where there is any large door opening, the threat of vehicular attack is always present.

Certain techniques exist for hardening and thus upgrading vehicle doors. Rubber tiers could be installed directly behind the outer vehicular door (with a portion below ground level) for greater penetration resistance, or a door clad

TABLE 6-1 Estimated Penetration Times for Standard Vehicle Doors

Barrier	Countermeasure	Countermeasure Weight (pounds)	Penetration Time (minutes)
Corrugated steel	Jet Axe, JA-I	20	0.8 ± 0.2
Hollow steel	Pry bar and 2 × 4 plank	23	0.9 ± 0.2
	Pry bar	15	0.2 ± 0.4
	Fire axe	10	3.8 ± 0.8
	Bulk explosives	10	About 1

Source: From the U.S. Nuclear Regulatory Commission.

with sheet metal could be used to resist vehicular penetration. Redwood could be inserted into a panel door to increase resistance to penetration by thermal tools. In this case, however, the increased weight necessitates the use of correspondingly upgraded hardware, which, as an added benefit, enhances protection of the door against tool and vehicular attack. Alternately laid steel channels welded together and covered by sheet metal could be used as a door and could provide significant penetration resistance.

Where lateral wall space is not a consideration, the use of a manual or mechanically actuated sliding door should be considered. The door should be constructed (or hardened) to the same standards and by the same methods as specified for personnel doors. In addition, the top runner track must be reinforced and a substantial, well-anchored channel must be provided for the bottom of the door to travel in.

The sliding door presents definite security advantages over those offered by the corrugated steel roll-up door. For example, the structural steel members needed to support a roll-up door adequately are of greater bulk and complexity than those required by the sliding door. The joints necessary in the corrugated steel roll-up door present a weakness in overall structure and are vulnerable to attack. By its very nature, the sliding door is a single, solid entity. Because of its method of mounting, it is almost impervious to forced entry by use of a pry bar, especially when the top track rail is hardened.

Aside from being rammed with a vehicle, the main vulnerability of the sliding door would be to pry against its opening edge. This method of attack can be forestalled by installation of several manually activated drop-pins similar to the familiar barrel bolt, although of much larger and sturdier construction. These drop into receiver holes drilled into the inner rail of the bottom track or into the floor. An intruder attempting to cut through these drop-pins would have to make a lateral cut the entire width of the door (unless able to determine the approximate location of the pins by either spotting the heads of their mounting bolts that protrude through to the outer door surface, or by simply estimating that the pins have been situated on and equidistant from the door's center line). To prevent this, drop-pins must remain undetectable from the outside of the door and spaced at random intervals along the lower door. While the upper track anchoring points ordinarily are subject to tool attack, their protection by a steel plate or apron on the outside, or attack side, of the door would discourage anyone concerned with affecting a stealthy entry.

The third type of vehicle door that may be encountered in a high-security installation is very similar to that used in the average homeowner's garage. This consists of a series of rigid panels joined together along their horizontal edges by hinges so that when the door is raised, it rolls up along a track and usually stores itself under spring tension, parallel to, but approximately 8 feet off, the floor. There is similarity between these doors only in a generic sense. The home garage door usually has panels constructed of tempered Masonite® or a similar product set into wooden framing, with each panel joined to those adjacent by three hinges and usually with a series of glass panes replacing one of the lateral panels. This door can be defeated with nothing more sophisticated than a rock or a shoe. Even without the glass, the panels can be quickly broken out of their support framing.

The high-security articulated vehicle door, however, is usually constructed of panels composed of a corrugated metal stiffener sandwiched between aluminum plates or special steel alloy panels. The hinges are often of the continuous or piano type and the track is reinforced to resist external force and carry the door's extra weight when in the retracted or stored position. As previously stated, however, this type of door is susceptible to vehicle attack or forced entry by lifting with a pry bar.

Vault Doors. By their purely functional design and often massive construction, vault doors instantly discourage attempts at forced entry by all but the most determined adversaries. This is probably the ultimate application of the psychology of maximum security as a deterrent. Prior to opting for the construction of a vault, however,

careful consideration must be given to the following questions:

1. What is the expected maximum period vault protection will be required?
2. Do federal, state, or local government regulations require vault protection of these assets?
3. Are the assets being protected of a size and configuration that makes their unauthorized removal extremely difficult without the use of heavy or special equipment not generally available in the area?
4. Can the asset being protected be rendered unusable by removal of key components? (Separate storage of these components would be required; however, the size of the resultant security system could be reduced with appropriate corresponding dollar savings.)
5. Will movement of the assets being protected be kept at a minimum?
6. Do large numbers of persons require daily access to these assets during the course of their duties?
7. Would theft of these assets have an adverse effect on
   a. The company's continued ability to remain in business (a trade secret of nonpatented process, material, machine, etc.)?
   b. The health and welfare of the general public?
   c. The environment?
   d. National security?
8. Will construction of a vault lower insurance premiums?
9. Can a vault be constructed within the existing facility without extensive renovation or reinforcement?
10. In the event of company growth, would the present facilities be sufficient to accept this growth and provide the room for expansion or would a move elsewhere be necessary?

Strong Room Doors. If, after considering the pros and cons of vault acquisition, it is decided that the cost of protection would be prohibitive in comparison to the benefits, serious consideration should be given to construction of a vault-type room or strong room.

A strong room is an interior space enclosed by or separated from other similar spaces by walls, ceiling, and floor constructed of solid building materials, with no windows and only one entrance. Strong room doors should be of heavy-gauge metal construction or of solid hardwood reinforced with a metal plate on the inside. Door louvers and baffle plates (if used) should be reinforced with 9-gauge, 2-inch square wire mesh fastened on the interior side of the door. Heavy-duty hardware should be used in constructing a strong room door; all screws, nuts, bolts, hasps, hinges, pins, and the like should be securely fastened. The door should be set into a suitable frame in the same manner as previously described for installation of personnel doors. Where air-conditioning or heating ducts pass over or through the strong room or where sewers or tunnels may pass under this space (and they are of a size and shape large enough to accommodate a small person), they should be equipped with personnel barriers. Duct barriers should be constructed of heavy-gauge wire mesh securely fastened to the duct by welding. For sewers and utilities tunnels, effective barriers can be constructed of steel bars or rods ¼ inch in diameter extending across the width of the pipe or tunnel with a maximum spacing of 6 inches between the bars. The ends of these bars or rods should be firmly anchored to prevent removal, and, where the vertical and horizontal bars or rods meet, they should be welded together. In effect, this forms very substantial grill work that cannot be easily defeated.

Emergency Doors. While some may argue that emergency doors have no place in a maximum-security setting, their use is mandated most of the time. If a facility is of a certain size or employs a certain number of people, it must by statute provide a specific number of emergency exits. In the maximum-security environment, these should be kept to the minimum required by law. Their number and location depend on many variables, such as the type of work performed in the building and the work space configuration (or partitioning) within the building. To ensure that emergency exits do not diminish the effectiveness

of the maximum-security measures in place, the following questions must be answered:

1. Where are the emergency exits located with respect to the assets being protected?
2. What type of emergency exit door (including hinges, locking mechanism, frame, anchoring, etc.) is installed?
3. Into what areas do the emergency exits allow personnel to pass?
4. Do the doors have alarms?

If particularly valuable or strategic material is processed or ordinarily handled near an emergency exit, the possibility of diversion of this material through the door is very real. It is relatively easy for a dishonest employee to hide quantities of the material during an emergency evacuation or drill and cache it outside the facility for later retrieval. The possibility must be considered.

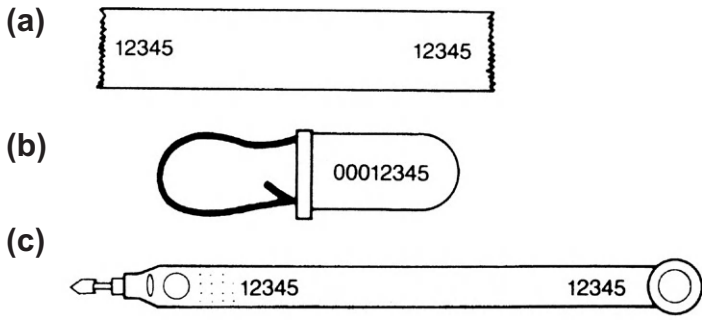
There are no hard and fast rules relative to the construction of emergency doors and hinges and methods of mounting. The obvious choice would be doors, hinges, and frames of construction and quality equal to the other security doors in use at a facility. It naturally follows that, if a high-security door is procured, the method of mounting should not negate the money spent on its purchase. The only element of an emergency exit over which there is little if any control is its locking mechanism. Most ordinances covering the use of emergency exits and devices are fairly specific in requiring the use of a panic bar locking mechanism. The type of panic bar usually encountered on emergency exit doors is most susceptible to defeat by an adversary using a simple wire hook or coat hanger. To maintain security of the exit, some people have chained or otherwise locked (from both sides) emergency exits. This can have disastrous consequences such as those experienced during the fire at the Coconut Grove nightclub in Boston, where nearly 500 lives were lost because the exit doors were locked.

Methods are available, however, to ensure that exit doors keep people out but allow the safe exit of those inside. One system provides overlapping sections fastened to stiles that meet and overlap when the door closes. The stiles close the gaps around the door so that prying tools cannot be forced through to trip the panic bar. None of the equipment is exposed, so would-be intruders cannot push it out of the way. When the panic bar is depressed, however, the barrier springs free and the door opens easily. As added security, the hinges are tamper resistant, which makes defeat by removing them quite difficult.

Another type of panic bar emergency device eliminates the bar that can be easily tripped and replaces it with a rim device that is not as likely to be snagged by a coat hanger.

At most facilities, emergency exits allow personnel to exit into parking lots, alleyways, or city streets. When evacuation is necessary, however, people should be channeled by physical barriers to a central assembly area that is under the control of the security department. Personnel should not be allowed to exit into a parking lot, alley, or street. To allow this could facilitate employee theft or diversion of the assets being protected or could lead to a breach in the security system by an insider who would allow accomplices to enter the facility and plunder it. In addition to employing physical barriers to move evacuating employees to a controlled safe area, the security department should be organized to provide some sort of monitoring of the evacuation process and routes to ensure that stolen or diverted material is not passed through or thrown over a fence to an accomplice or for later retrieval.

Alarms on emergency exit doors should be mandatory. Not only should the door have a locally annunciating alarm, but it must be tied into the facility's central alarm station. In this way, each alarm system backs up the others. To ensure positive performance, these alarm systems must be periodically checked. It is suggested that a check at least twice a day of both systems be implemented. In addition, each emergency exit door should be affixed with a tamper-indicating seal (or seals; Figure 6-4) and these should be checked each time the alarm system is checked.



Roofs

FIGURE 6-4 Tamper-indicating door seals: (a) serially numbered tape type, (b) serially numbered heavy wire and plastic type, and (c) serially numbered plastic strip type.

ROOFS

In arriving at a design for a maximum-security roof (or ceiling), the most obvious and simplest solution would appear to be to use the same specifications and technology employed in the construction of the high-security walls in this space or building. However, some considerations must be made that are not instrumental in wall design:

1. How much loading will this roof or ceiling be subjected to?
2. If this is a ceiling in a multistory facility, will the space directly above the protected area be covered by a trained and suitably equipped member of the security force or by a sophisticated alarm system that annunciates locally and at a remote monitoring station staffed around the clock?
3. Will the integrity of the roof or ceiling be broken by piping, ductwork, or access hatches?
4. Will any portion of the roof be accessible from outside the protected area or, conversely, grant access outside the protected area from inside it?
5. Will the roof or ceiling have alarms, monitored by security officers or CCTV, equipped with adequate lighting to permit proper assessment, and not provide places of concealment for intruders, such as air-conditioning units, exhaust fan hoods, or smoke pipes?

These and many more site-specific questions must be worked out between the building architect or room designer and the person responsible for ensuring the degree of security necessary. Officials involved in the preliminary planning stages of the construction of a new facility or upgrading of an existing one into the maximum-security class must include the company security director. This individual should be prepared to discuss these matters with the staff and obtain input from the personnel who are responsible for making sure that the system works. If the facility is part of a corporation that may have installations of this type in other locations, a visit to one or more of these sites by the security staff pays handsome dividends in avoiding mistakes that may plague others. Careful and imaginative planning eliminates costly (and embarrassing) oversights that may require considerable time, effort, and expense to rectify.

The prime requisite of any roof in a maximum-security setting is its ability to withstand or defeat attempts at forced entry. The roof most commonly selected is usually constructed of poured concrete, approximately 5½ inches thick with steel reinforcing rods on 8 × 12-inch centers embedded in the center of the concrete slab. In tests of resistance to forced entry, it was found that 4 pounds of bulk explosives and 20-pound bolt cutters required only 2.8 ± 0.4 minutes to effect penetration. Another type of roof construction

often found in industry and government buildings consists of 16-gauge sheet metal placed on ribbed steel decking, covered by 2 inches of insulation followed by a final covering of a ½ inch of asphalt and gravel. Using a 10-pound fire axe and a 5-pound shovel, penetration was achieved in 2.3 ± 0.7 minutes. In a test of this same type of roof construction, 20 pounds of Jet-Axe JA-I charge and equipment affected penetration in 0.8 ± 0.2 minutes. The conclusion reached in the study from which these results are drawn is that, despite quite a few variations in the types of materials and the manner in which they may be assembled, all can be defeated in about a minute with a few pounds of appropriate explosive. The obvious answer, therefore, is to construct the best roof possible but prevent anyone from reaching it by establishing a protected area around the building, then providing adequate assessment capabilities, alarms, and the like to detect anyone who may manage to penetrate the protected area.

If the construction of a strong room is being considered within an existing maximum-security setting, there are several combinations of commonly available materials from which to fabricate a homogeneous roof or ceiling that provides significant resistance to forcible entry.

The creation of this roof or ceiling is well within the capabilities of any commercial carpenter with assistance from a sheet metal shop. In tests conducted by the Civil Engineering Laboratory of the Navy Construction Battalion Center, the best composite material consists of 0.1-inch sheets of 6061-T6 aluminum over ½-inch plywood on both sides of a 19-gauge 304 stainless steel sheet. In laboratory tests, a panel constructed in this manner was subjected to attack by a 7¼-inch circular saw equipped with a metal cutting blade and an oxy-acetylene torch; the average rate of linear progression was 3.06 inches per minute. Switching over to the circular saw with metal cutting blade, 22 seconds passed without complete penetration. In all cases, large quantities of smoke were generated, as the saw blades and stainless steel sheet became extremely hot. Subsequent tests indicated that an abrasive blade on the saw was ineffective.

To defeat attempts simply to disassemble the roof when the composite is assembled into standard-sized panels and then used as conventional building materials, the substrate should be laid in a random pattern to avoid the neat layering of edges through all the various materials. The components can be bonded together through the use of nuts and bolts, screws, tempered screw-nails, or ringed nails; however, the nuts and bolts should be peened to prevent removal and the heads of the screws should be ground for the same purpose. Although someone could shear off the nail heads, the holding action of the nail shanks would still present a formidable task to anyone inclined to attempt to peel the roof. If this type of composite is used, it must be remembered that it would be covered by insulation and probably several different layers of weatherproof roofing. This additional material would add substantially to the penetration resistance of such a roof. Its use is not recommended, however, in the construction of a roof that has no alarm, is not easily visible to the guard force or well lighted, or is close to or part of the protected area perimeter. As previously indicated, this material would be suitable inside an already protected installation or could be used in small, low buildings located well within a protected area.

Upgrading Existing Roofs. When the company security department is faced with the task of upgrading an in-place facility, the task becomes many times harder. The installation of alarms, lights, doors, walls, gates, and many other security responsibilities must be considered.

Before upgrading the roof of an existing facility, the security director must climb up there and have a firsthand look. What can be seen? Do fire escapes allow access to the roof? Are there roof hatches, skylights, ducts, piping, air-conditioning units, strong and firmly attached downspouts, or coamings (which could anchor a grappling hook)?

Once you have made an assessment of the roof's liabilities, consult the individual responsible for maintaining plant services (usually the chief of maintenance of the physical plant) and ascertain which of these potential access points

are essential to plant operations. If the plant site is an old building, many of these potential problems can be eliminated as the elements are nonfunctional, having been replaced by more modern equipment, but remain in place simply because they plug a hole that would be left in the roof by their removal. Once a decision is made as to which appurtenances can be removed, the subsequent hole should be rehabilitated so that the physical integrity and strength of the repair is no less than that of any other part of the original and undamaged roof structure.

Low flat roofs that might be susceptible to scaling through use of a grappling hook should have shielding installed behind the coaming to prevent the hook from finding a secure anchor. This need not be anything more exotic than panels of heavy-gauge sheet metal. These can be anchored to the lip of the coaming and roof and angled back toward the roof to form an inclined plane up which the hook rides right back over the edge (Figure 6-5).

Another possibility that may be worthy of consideration, especially for facilities situated in remote areas, is attack by helicopter. If the roof of the main building or the building that would be the attacker's objective is flat, and thus suitable for landing a helicopter, or even if it is not flat but is suitable for landing an attack force from a hovering helicopter, consideration should be given to installing one or more tall, lightweight metal light poles to the roof. These prevent the helicopter from landing or coming close enough to the roof to discharge personnel. These poles could also support area floodlights that would light the protected area and rooftop. In addition, flagpoles, radio communications antennas, tall chimneys and exhaust stacks, or guy wires prevent this type of attack.

FLOORS

In most buildings, the floor is probably the least thought out part of the total security package. It exists to provide a smooth, dry working surface and as a base on which the building may be erected floor by floor. True? Ordinarily, this would be a good thumbnail description of the purposes of flooring; however, in a maximum-security installation, the same amount of thought devoted to the wall and roof design must be allotted to the floor. A typical floor is usually constructed of poured concrete, 6–8 inches thick, and reinforced with rebar steel rods or 6-inch square mesh of no. 10 wire. Floors constructed in this manner are adequate for most facilities; however, penetration time by one or two adversaries using explosives, sledgehammers, and bolt cutters in any combination averages 2–4 minutes.

This penetration time does not take into account the time spent in arriving at the site, setting up for the penetration, retreat time

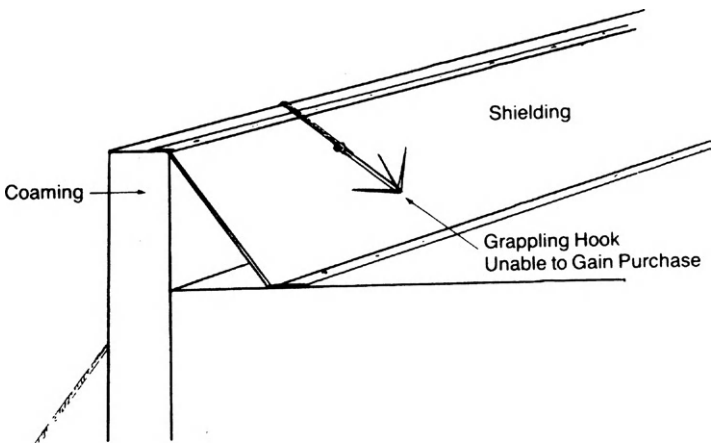


FIGURE 6-5 Grappling hook shielding.

(if explosives are to be used), and crawl-through. If the target is located in a multistory building, the attempted penetration may come from above or below; therefore the floor in the space above the target site must provide an amount of resistance equivalent to that of the other security features.

How can existing floors similar to those previously described be afforded an additional measure of penetration resistance? The most obvious answer would be to increase the floor's thickness by adding additional layers of rebar, reinforcing wire, and poured concrete. This simplistic solution should not be implemented lightly, as the addition of what may amount to quite a number of tons of weight to a structure that was not originally designed for this additional weight could present a very real personnel safety hazard. If this is the only feasible solution, a competent engineering firm should analyze the situation and design the necessary additional supporting columns or beams to ensure an adequate margin of safety.

If the cost of accomplishing a complicated building redesign and renovation as briefly described here is not possible, an alternative may be to relocate the objective to a ground floor or perhaps even into a below-ground location. If the target is relocated to ground level, it should be placed away from exterior walls, preferably toward the center of the structure with several intervening walls between it and any exterior wall (i.e., layered; see Figure 6-2).

If a basement or utility space is under the site selected for relocation, it should be sealed off or provided with sophisticated alarms to preclude entry from that point.

An interesting method of tremendously increasing the penetration resistance of a wall that is adaptable to floors (and ceilings) would be to anchor steel I-beams into the concrete walls, interlocking as many additional beams as necessary across the width of the floor (or ceiling). These beams are covered with a simple overlaid wooden floor, which is tiled or carpeted as required. Figure 6-6 shows how this hardening method would appear in cross-section. Properly installed, the I-beams would increase the penetration resistance time to approximately 2–4 hours. The additional weight, however, restricts the use of such a hardening or protection method to new construction or a facility in which the proper steps have been taken to ensure that the total system has been properly engineered.

FENCES

Fences are used to

- Define a particular area
- Preclude inadvertent or accidental entry into the area
- Prevent or delay unauthorized entry
- Control (or channel) pedestrian and vehicular traffic

In a maximum-security setting, fences are not the ideal barrier (Table 6-2); walls of solid construction should be used for these purposes. It is recognized, however, that walls are often undesirable or impractical, and fences are the most viable alternative.

The type of fence used in a maximum-security setting should be chosen after careful analysis of many factors. Based on determination of the objectives it will serve, these additional questions should be answered:

1. Will one fence be enough or will two or more in a series be required?
2. Will there be vehicle barriers in conjunction with the fence?
3. How far will the fence be from the area of chief concern?
4. What will be the closest area of concealment to the fence?
5. Will the fence have alarms?

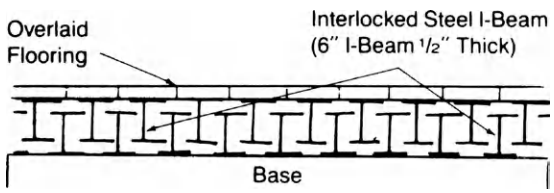


FIGURE 6-6 I-beam application to floors. (Courtesy of U.S. Army Material Systems Analysis Activity.)

TABLE 6-2 Penetration Aids

Item	Description	How Used
Canvas sheet	6 × 8-foot folded sheet	Thrown over top of fence to aid climbing
Cutters	Bolt cutters, wire cutters, tin snips	To cut fence fabric, barbwire, or tape
Steps	18-inch iron rods bent into step form	Hooked into fence fabric and used as climbing aids
Wire hooks	6- to 12-inch lengths of stiff wire bent into hooks	To hold barbed tape to fence to aid climbing
Long hooks	3-inch rods bent into hooks	To pull down barbed tape topping to aid climbing
Ladder	7-foot stepladder	To jump over fence
Extension ladder	20-foot ladder hinged in the middle to form an A	To cross over combination barbed tape-fence barriers
Pry bar	10-foot 2 × 4 or piece of 2-inch pipe	To lift fence fabric to aid crawling underneath fence
Plywood	4 × 8-foot sheet of $^3/_8$-inch plywood	To put over barbed tape to aid crossing
Carpet	4 × 15-foot heavy carpet rolled up on a 5-foot 4 × 4	To throw over fence to aid climbing
Plank	Two 8-foot 2 × 2 planks with a nail in one end	To lift caret roll over fence

Source: From the U.S. Department of Commerce, National Bureau of Standards.

Environmental conditions certainly affect the design of a fence system and should be considered:

1. Will erosion under the fence be a problem?
2. Will corrosion of the fence be a problem?
3. What natural features or vegetation around the fence might interfere with detection or assessment of activity in the area?

Selection of the kind of fence does not stop at a choice of fabric; decisions must be made as to height, the means of anchoring the posts and bottom, and the type of topping. If two or more fences are to be installed, what, if anything, will be placed between them and what will be the distance between them? Finally, considering the kinds of tools likely to be required for penetration, what will be the total penetration time for all fences and obstacles? Once these questions are answered, planning can commence. The type most frequently encountered is no. 11 American wire gauge or heavier, with 2-inch mesh openings, 7 feet in height, topped by 3 strands of barbwire or barbed tape evenly spaced 6 inches apart and angled outward 30–15 degrees from the vertical.

This type of fence can be breached in 4.3 ± 0.3 seconds using no material aids, but with the assistance of one person not crossing. To increase the penetration time of this fence to 8.4 ± 1 seconds, it is necessary to install V-shaped overhangs with concertina barbwire or barbed tape inside the V. The types of fences described can be driven through in a light pickup truck in 2 ± 1 seconds with no significant damage to the truck.

Less frequently encountered fences include the V-fence, which consists of 3-inch posts set at an angle of 60° in 30-inch diameter by 24-inch high concrete footings 12 inches below grade. The posts are in 10-foot centers and staggered 5 feet front to back. The chain-link mesh is 10 feet high with a cable installed at the top. A corrugated steel sheet is placed on the outside posts to prevent them from being crawled under. Nine rolls of general purpose barbed tape obstacle (GPBTO) are used inside the V to delay crawl-through.

All rolls are secured to the chain-link mesh with wire ties. Cutting through this fence takes about 4 minutes. Climb-over takes only 40 seconds, using ladders and bridges as breaching aids. This fence can be equipped with razor ribbon instead of GPBTO, with a second sheet of corrugated steel attached to the inside posts to form a V-shaped trough filled with 2- to 5-inch rocks and 9-inch diameter telephone poles, and with 6 rolls of barbed tape concertina. Thus outfitted,

it offers a penetration resistance of 10 minutes for digging and crawling under. Climb-over times are similar to those of the V-fence previously described. While personnel penetration cannot be prevented, breaching by a vehicle is almost impossible for the latter type of V-fence.

Regardless of how elaborate fences may be, they still offer only a modicum of security. Fences are necessary, but investment in this area should be kept to a minimum as the money can be better used on other components of the total system.

In a maximum-security environment, certain things must be kept in mind regarding the use of fences. Height should be a preliminary consideration. The higher the fence, the better is the chance of defeating a climb-over by personnel using the simplest breaching aids. Whenever a fence is used in a maximum-security system, the method of anchoring it is very important. No matter how sophisticated the fence may be, if the fabric can be pried from ground level using a 2 × 4 or similar breaching aid, it is nearly useless.

According to the *Barrier Technology Handbook*,

> *The time required to go under a fence is only slightly longer than the time required to climb a fence without a barbed tape topping but is significantly shorter than the time required to climb a fence with a barbed tape topping when only limited aids are used.*

Penetration time can be doubled by the addition of a bottom rail (Figure 6-7). Many fences are constructed so that the bottom of the fabric touches the ground or is no more than 2 inches above ground level. Without some method of anchoring this fabric, crawl-under is quite simple. If cost is no obstacle, burying the lower portion of the fabric (about 3–6 inches) in concrete would virtually preclude crawl-under. Another alternative would be to anchor the bottom of the fence fabric with 3-inch reinforcing rods to precast concrete sills 8½ feet long, 10 inches high, and 3 inches wide. Each sill is buried under the fence fabric, between posts, with 3 inches of sill above ground and the reinforcing rods from the sill bent around the fence fabric. This method is effective because it takes less time to cut through or climb over the fence than it does to separate the fabric from the reinforcing rods.

Topping a fence with barbwire or barbed tape is another consideration. The U.S. Nuclear Regulatory Commission (NRC) requires protected area fences to be topped with at least three strands of barbwire angled outward at a 30–45° angle. As previously mentioned, this particular topping does very little to preclude climb-overs. A somewhat better topping is GPBTO, often called *razor ribbon*. It is intimidating in appearance and thus offers a psychological deterrent to less than determined adversaries. In actuality, however, the use of breaching aids generally improves penetration times for barbed-tape-topped fences. The *Barrier Technology Handbook* states:

> *The fastest penetration times for barbed-tape-topped fences were achieved when a piece of carpeting was thrown over the fence. The carpet was made by nailing the end of 4 × 15-foot long heavy carpet to a 5-foot long 4 × 4 and then rolling the carpet around the 4 × 4.*

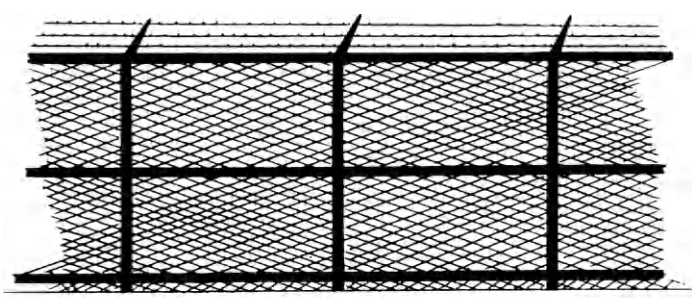


FIGURE 6-7 Bottom fence rail.

Generally, the addition of any barbwire or barbed-tape topping does not significantly increase penetration resistance. An intruder who is discouraged from climbing over and crawling under will probably choose to go through the fence.

Cutting through the fence generally takes more time than climbing over or crawling under. Once again, the fact that the bottom portion of the fabric is securely anchored increases penetration time. If the bottom is not anchored, "it takes only a single row of approximately 12–15 cuts to make a man-sized opening. Anchoring the fence in concrete doubles the cutting time." To double the cutting time through chain-link fence, it is necessary to fasten another layer of fabric to the inside of the fence.

Yet another way of increasing cut-through time would be to interlace metal or wood lattice in the fabric. This technique, however, significantly reduces visibility and should not be used when the fence is the single component of a perimeter protection system. (Fences should never be the single component of a perimeter protection system in a maximum-security environment.)

Entry and Exit Points

Entry and exit must be considered when erecting a security fence. The first criterion should be that the integrity of all gates and doors be the same as or better than that of the fence in which they are installed. Entry and exit points should be kept to the minimum number necessary to maintain compliance with governmental or company mandates.

Gates should open out if at all possible. Many swing in and out and should be modified accordingly. They should be equipped with a jam or frame to strengthen the integrity of the opening. The most common types are swing gates and sliding gates with variations.

Most vehicular gates have access roads aimed directly at them, thus facilitating vehicle intrusions. Penetration resistance of most fabric-type gates is equivalent to that of the fence in which they are installed. Vehicle drive-through is easier at a gate than at any other part of the fence. The use of metal doors set in jambs rather than gates offers a somewhat higher degree of penetration resistance but the cost is usually not worth it, although for emergency fence doors this should be mandatory. For any emergency door in a perimeter fence, opening should be facilitated by a panic bar on the inside. Emergency doors should be locked and the panic bars installed so that an intruder cannot use the bar to open the door from the outside.

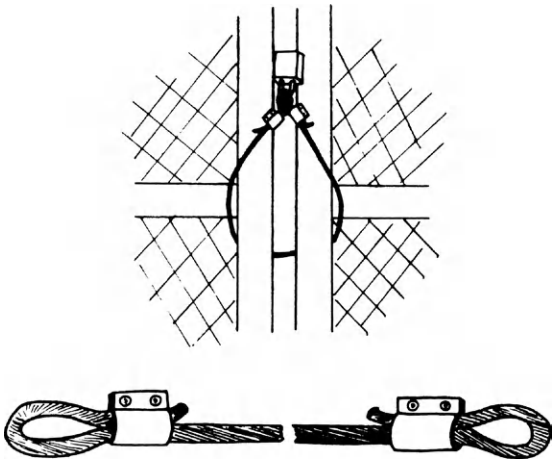


FIGURE 6-8 Bridle.

Another method of controlling pedestrian traffic through fences is by use of turnstile gates. Penetration time (by deactivating electrical controls or forcible entry) is approximately 1 minute. When installed in a common chain-link fence, an adversary would probably choose to breach the fence rather than the turnstile gate.

The weak link in a gate is usually the hardware: hinges and locks. Fence gate locks should be accessible only from the inside. Built-in locks depend on fence alignment for effectiveness and should be supplemented with a piece of case-hardened or stainless steel chain and padlock. The chain should be wrapped around the fence post and gatepost until it is as tight as possible, and padlocked; no slack should be left in the chain. Where possible, stainless steel cable should be used, as it tends to flatten out when attacked with bolt cutters and is somewhat difficult to defeat. A bridle can be made from ⅜- to ½-inch stranded stainless steel cable, looped on both ends using Nicopress fasteners (Figure 6-8).

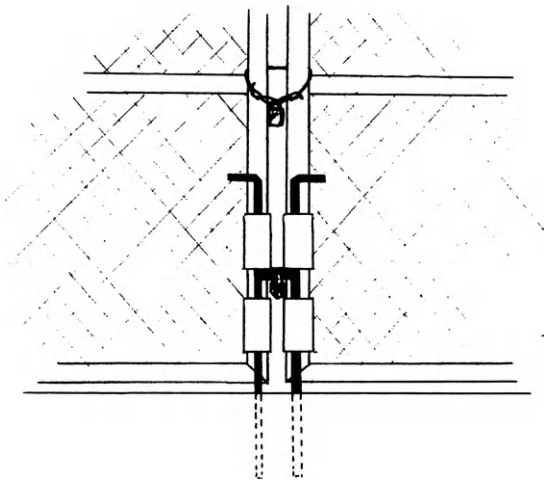


FIGURE 6-9 Double-leaf gate drop bolts.

Bridles can be used in conjunction with case-hardened padlocks for a variety of purposes.

A double-leaf swing gate should be securely anchored where both leaves meet by a solid foot bolt, several feet long, on each leaf that is dropped into a steel anchoring hole in the ground (Figure 6-9). The addition of a chain or cable and padlock enhances the gate's security.

Because fences are not the ideal physical barriers in a maximum-security environment, their usefulness is limited. Their primary function should be to simply define a particular area.

WALLS AND MOATS

In designing a maximum-security perimeter barrier system where cost is no object, the most penetration-resistant structure is a thick, high wall. Walls, however, do not allow free visual access to the area outside. A possible alternative is the modern equivalent of the medieval moat.

It completely surrounds the protected area, and all entry and exit points are bridged with fixed or movable structures. These points can be kept to the absolute minimum and controlled around the clock. They can also be equipped with methods of preventing breach by ramming with a vehicle.

The moat would be the dry type and equipped with a suitable drainage system. It would be at least 8 feet deep and measure a minimum of 10 feet from edge to edge. To increase protection, a standard chain-link fence topped with an outrigger equipped with three strands of GPBTO would be positioned at the inner edge. This would be attached in such a way that there would be little or no lip that could be used to support a ladder or serve as a working platform for someone attempting to cut through the fence fabric. The fence posts would be a minimum of 3 inches in diameter and concrete filled. Top rails would not be used. The strong fence posts would maintain the longitudinal rigidity required, but by omitting the top rail stiffener, a degree of instability is introduced that would increase protection by making it difficult for someone to secure a good anchor point for a bridge or from which to work to penetrate the area.

The bottom edge of the fence fabric would be embedded in the concrete at the time the moat lining is poured to prevent entry by prying up the fabric and crawling under.

The specification of moat depth and width can be reached only when integrated into the total barrier design. A minimum depth of 8 feet is recommended as this would require a larger ladder to reach from the moat bottom to the top of the fence. Such a ladder would be bulky and difficult to maneuver and could not easily be hidden if it must be brought to the planned penetration site on foot. An 8-foot depth also serves as a definite deterrent to anyone contemplating penetration by crashing through the fence with a vehicle. Any commonly available tracked vehicle, including a bulldozer, would be unable to climb out of the moat due to this depth and the 90° wall angle. A minimum width of 10 feet is recommended, because this would preclude the use of uncomplicated bridges such as a 4 × 8-foot sheet of ¾-inch plywood. To prevent a ladder (modified by the addition of hooks or steel rods to one end) from being used as a bridge by hooking or inserting the modified end into the fence, an aluminum or galvanized steel sheet would be attached to the outside of the fence to a height of 3 feet. This ladder could still be used as a bridge by hooking it into the fence fabric above this plate, but

the angle and the unsteadiness would provide a very unstable work platform. The easiest way to bridge this type of perimeter barrier would be with a 20-foot extension ladder modified so that the upper end has a hook attached to the end of each leg. To use it, the ladder would be extended to its full height then allowed to fall across the moat so that the hooks would fall behind the top of the fence fabric. Once the hooks were in position, the ladder would form an inclined plane over which the adversaries could climb or crawl and drop to the ground inside the protected area.

This type of entry can, however, be defeated by a double moat system, which is nothing more than a second 8 × 10-foot (or larger) moat immediately adjacent to the first with the previously specified fence installed between them on a 12- to 15-inch-thick reinforced concrete wall. The fence would be topped with a Y-type of barbed tape standoff with concertina tape installed in the center of the Y as well as on either side of the outrigger arms.

On either fence, a motion detection system would be required along with a detection system located between 10 and 15 feet beyond and parallel to the second moat. To prevent the inadvertent entry of personnel and wildlife, an outer perimeter chain-link fence 8 feet high and topped with three strands of GPBTO could be installed. Depending on the amount of property available, this fence would be located a minimum of 25 feet from the outer edge of the first moat.

In our example, *cost is not a factor*; the objective is to use fencing and other physical obstacles as a first line of defense. As previously mentioned, our preference is the use of walls rather than fences.

Topography

The natural deterrence offered by topography, while often of limited value, should be taken into consideration when designing or upgrading a facility to the maximum-security level. Rivers and other large bodies of water, swamps, escarpments, deserts, and so forth are all examples of natural obstacles that may be used in various ways.

Probably the most famous examples of the optimal use of natural barriers were the prisons on Alcatraz Island in California and the French penal colony on Devil's Island located off the coast of (then) French Guiana. The physical barriers used to contain the prisoners in these facilities were usually enough to discourage escape attempts. Even if they might be defeated, however, the escapee was still left with no way off the island except by using materials at hand or (in the case of Alcatraz) attempting to swim to freedom. Although both prisons were in operation for many years, only a few escapes were ever successful.

When a facility has a river or other large body of water as a boundary, the natural obstacle may be used in conjunction with more traditional fences as a deterrent. The clear view of the approach route across these areas would discourage an adversary from attempting an approach from that direction, especially if faced with sophisticated alarms and barriers around the objective. In a remote or isolated area, a river or large body of water abutting the site could also serve as adversary approach or escape routes, turning these nominal topographic barriers into liabilities against which additional protection means or procedures must be provided.

The advantage offered by a desert environment is similar to that provided by a natural water barrier. As with water obstacles, the possibility of an unseen approach across a barren landscape is very slim. The advantages of isolation and early detection are outweighed by the fact that approach or escape might be accomplished across the very feature that seems to offer some degree of protection, from any direction.

Swamps, while not usually a consideration in a maximum-security setting, could conceivably be encountered. The principal advantage offered by marshy terrain is its impenetrability to usual forms of ground transportation. The most practical setting for a facility in a swampy area would be at the center of the swamp with only one access road. In the event of successful penetration of the facility, this access road could be blocked to contain the adversaries until outside assistance arrives at the scene.

The security offered by a deep forest should also be considered. When a facility is located in a remote area of dense forest, with very limited and controlled access routes, this remoteness discourages all but the most determined adversaries. As with the natural barriers provided by swamps, forest locations require adversaries to forego the usual methods of transportation when access routes are limited and controlled. This might mean they have to walk in, carrying all the equipment and arms they believe necessary for the successful completion of their mission. In addition, their escape plan must be structured to require, as the last resort, escape by foot. Depending on the remoteness of the objectives, the terrain to be encountered, and the climatic conditions prevailing, these difficulties, when considered above and beyond the resistance to be expected from the onsite security personnel, could force the adversaries to choose another course of action and shift their attention to a more vulnerable target.

In summary, natural barriers may be efficiently incorporated into a total security system only when effective, round-the-clock monitoring of these approach areas by a security guard or CCTV system is provided. Structural barriers physically and psychologically deter and discourage the undetermined, delay the determined, and channel the flow of traffic through proper entrances.

REFERENCES

[1] Barrier penetration database. Revision 1. Upton, NY: Brookhaven National Laboratory; 1978. p. 17.

[2] Barrier penetration database. Revision 1. Upton, NY: Brookhaven National Laboratory; 1978. p. 18.

[3] Hardening existing SSNM storage facilities, preliminary report. Aberdeen, MD: U.S. Army Material Systems Analysis Activity; 1979. p. 33.

[4] Barrier penetration database. Revision 1. Upton, NY: Brookhaven National Laboratory; 1978. p. 15.

[5] Hardening existing SSNM storage facilities, preliminary report. Aberdeen, MD: U.S. Army Material Systems Analysis Activity; 1979. p. 31.

[6] Technical memorandum No. 61–78–9. Port Hueneme, CA: Civil Engineering Laboratory, Naval Construction Battalion Center; 1977.

[7] Barrier technology handbook, 77–0777. Albuquerque, NM: Sandia Laboratories; 1978.

[8] Barrier penetration database. Revision 1. Upton, NY: Brookhaven National Laboratory; 1978. p.17.

[9] Barrier technology handbook, 77–0777. Albuquerque, NM: Sandia Laboratories; 1978.

[10] Barrier technology handbook, 77–0777. Albuquerque, NM: Sandia Laboratories; 1978.

[11] Barrier technology handbook, 77–0777. Albuquerque, NM: Sandia Laboratories; 1978.

[12] Barrier technology handbook, 77–0777. Albuquerque, NM: Sandia Laboratories; 1978.

[13] Technical memorandum No. 51–78–04. Port Hueneme, CA: Civil Engineering Laboratory, Naval Construction Battalion Center; 1977.

[14] Hardening existing SSNM storage facilities, preliminary report. Aberdeen, MD: U.S. Army Material Systems Analysis Activity; 1979. p. A-6.

[15] Hardening existing SSNM storage facilities, preliminary report. Aberdeen, MD: U.S. Army Material Systems Analysis Activity; 1979. diagram 5.

[16] Hardening existing SSNM storage facilities, preliminary report. Aberdeen, MD: U.S. Army Material Systems Analysis Activity; 1979. pp. 78–79.

[17] Barrier penetration database. Revision 1. Upton, NY: Brookhaven National Laboratory; 1978. p. 8.

[18] Hardening existing SSNM storage facilities, preliminary report. Aberdeen, MD: U.S. Army Material Systems Analysis Activity; 1979. p. 8.

[19] Hardening existing SSNM storage facilities, preliminary report. Aberdeen, MD: U.S. Army Material Systems Analysis Activity; 1979. p. 9.

[20] Hardening existing SSNM storage facilities, preliminary report. Aberdeen, MD: U.S. Army Material Systems Analysis Activity; 1979. p. 9.

[21] Hardening existing SSNM storage facilities, preliminary report. Aberdeen, MD: U.S. Army Material Systems Analysis Activity; 1979. p. 8.

[22] Hardening existing SSNM storage facilities, preliminary report. Aberdeen, MD: U.S. Army Material Systems Analysis Activity; 1979. p. 77.

[23] Barrier technology handbook, 77–0777. Albuquerque, NM: Sandia Laboratories; 1978. paragraph 3.5.4.

[24] Barrier technology handbook, 77–0777. Albuquerque, NM: Sandia Laboratories; 1978. p. 79.

[25] Barrier technology handbook, 77–0777. Albuquerque, NM: Sandia Laboratories; 1978. paragraph 3.7.4.3.

[26] Barrier technology handbook, 77–0777. Albuquerque, NM: Sandia Laboratories; 1978. p. 80.

CHAPTER

7

Use of Locks in Physical Crime Prevention*

James M. Edgar, William D. McInerney, Eugene D. Finneran, John E. Hunter

LOCK TERMINOLOGY AND COMPONENTS

The effectiveness of any locking system depends on a combination of interrelated factors involved in the design, manufacture, installation, and maintenance of the system. A prevention specialist needs to understand the weaknesses and strengths of the various systems, and know how each must be used to achieve maximum benefit from its application. This requires a thorough understanding of the inner workings of the various types of locks. It is not sufficient to know what a good lock is in someone else's opinion. A good lock today may not be as good tomorrow as technology improves and manufacturers alter their designs and production techniques. A lock that is excellent in some applications may be undesirable in others. Knowledge of the basic principles of locking systems will enable a preventions specialist to evaluate any lock and determine its quality and its effectiveness in a particular application.

*Permission obtained from National Crime Prevention Institute, School of Justice Administration, University of Louisville, Kentucky.

KEY-OPERATED MECHANISMS

A key-operated mechanical lock uses some sort of arrangement of internal physical barriers (wards, tumblers) that prevent the lock from operating unless they are properly aligned. The key is the device used to align these internal barriers so that the lock may be operated. The lock is ordinarily permanently installed. The key is a separate piece, which is designed to be removed from the lock to prevent unauthorized use.

Three types of key-operated locks will be introduced in this section: disc or wafer tumbler, pin tumbler, and lever.

Tumbler Mechanisms

A tumbler mechanism is any lock mechanism having movable, variable elements (the *tumblers*) that depend on the proper key (or keys) to arrange these tumblers into a straight line, permitting the lock to operate. The tumbler, which may be a disc, a lever, or a pin, is the lock barrier element that provides security against improper keys or manipulation. The specific key that operates the mechanism (called the *change key*) has a particular combination of cuts, or bitings, which match the arrangement

of the tumblers in the lock. The combination of tumblers usually can be changed periodically by inserting a new tumbler arrangement in the lock and cutting a new key to fit this changed combination. This capability provides additional security by protecting against lost or stolen keys.

Tumbler mechanisms and the keys that operate them are produced to specifications that vary with each manufacturer and among the different models produced by each manufacturer. These specifications are known as the *code* of the lock mechanism. The coding for each mechanism provides specifications for both the fixed and variable elements of the lock assembly. Fixed specifications include:

- The dimensions of each of the component parts of the lock and the established clearance between each part (e.g., the size and length of the key must match the size and depth of the keyway).
- The spacing of each tumbler position and their relation to each other (Figure 7-1).
- The depth intervals or increments in the steps of each cut or biting (Figure 7-2).

The relationship between the dimensions of the tumblers and the biting on the key is shown for a typical pin tumbler mechanism in Figure 7-3. These codes provide a locksmith with dimensions and specifications to produce a specific key to operate a particular lock or to key additional locks to the combination of a particular key.

The different arrangements of the tumblers permitted in a lock series are its *combinations*. The theoretical or mathematical number of possible combinations available in a specific model or type of lock depends on the number of tumblers

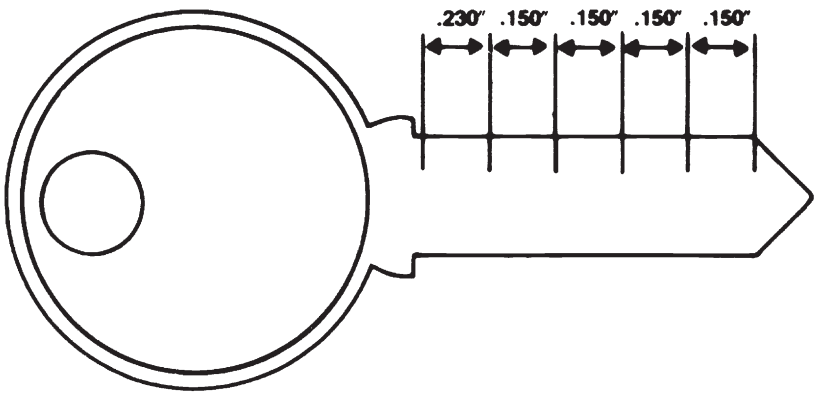


FIGURE 7-1 The spacing or position of each cut on the key is a fixed dimension corresponding to the position of each tumbler in the lock.

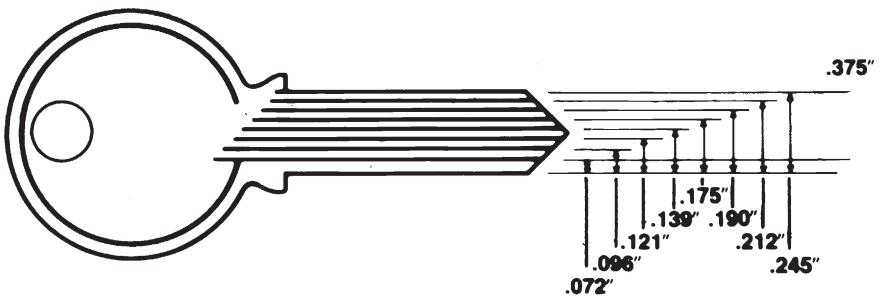


FIGURE 7-2 The depth interval (increment) of the steps of each cut or biting is a fixed dimension.

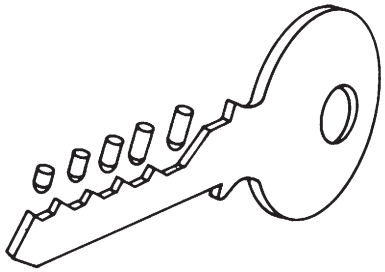


FIGURE 7-3 The depth of each cut corresponds to the length of each tumbler in the lock.

used and the number of depth intervals or steps possible for each tumbler. If the lock had only one tumbler, which could be any of 10 lengths, the lock would have a total of 10 combinations. If it had two tumblers, it would have a possible total of 100 (10 × 10) combinations. With three tumblers, 1000 (10 × 10 × 10) combinations are possible. If all five tumblers were used, the lock would have a possible 100,000 combinations. The number of mathematically possible combinations for any lock can be determined by this method.

Due to a number of mechanical and design factors, however, not all of these theoretically possible (implied) combinations can actually be used. Some combinations allow the key to be removed from the lock before the tumblers are properly aligned (shedding combinations)—something that should not be possible with a properly combinated tumbler lock. Others, such as equal depth combinations, are avoided by the manufacturers. Some combinations result in a weakened key that is prone to break off in the lock. Others are excluded because the space from one cut in the key erodes the space or positioning of adjacent cuts. The combinations that remain after all of these possibilities have been removed are called *useful combinations*. The useful combinations, which are actually employed in the manufacture of the lock series, are the basis for the *biting chart* that lists the total combinations used in a particular type of model or lock. When other factors are equal, the more combinations that can actually be used in a lock, the greater the security of the lock. Total useful combinations range from one for certain types of warded locks to millions for a few high-security tumbler key mechanisms.

Disc or Wafer Tumbler Mechanisms

Disc tumbler mechanisms consist of three separate parts: the keys, the cylinder plug, and the cylinder shell (or housing; Figure 7-4). The plug contains the tumblers, which are usually spring-loaded flat plates that move up and down in slots cut through the diameter of the plug. Variably dimensioned key slots are cut into each tumbler. When no key is inserted or an improper key is used, one or more tumblers will extend through the sides of the plug into the top or bottom locking grooves cut into the cylinder shell, firmly locking the plug to the shell. This prevents the plug from rotating in the shell to operate the lock. The proper change key has cuts or bitings to match the variations of the tumblers. When inserted, the key aligns all of the tumblers in a straight line at the edge of the cylinder plug (the *shear line*) so that no tumbler extends into the shell. This permits the plug to rotate.

Disc mechanisms generally provide only moderate security with limited key changes or combinations. Depth intervals commonly used are from 0.015 to 0.030 inches, which permit no more than four or five depths for each tumbler position. Some models use as many as six tumblers. The more commonly found five-tumbler mechanism, which allows five depth increments for each tumbler position, would have a maximum of 3,125 implied combinations. The number of useful combinations would, of course, be considerably fewer for the reasons indicated earlier. Some added security is provided by the common, although not universal, use of warded and paracentric keyways, which help protect against incorrect keys and manipulation. Nevertheless, most of these locks may be manipulated or picked fairly easily by a person with limited skills. In addition, the variations cut into the tumblers can be *sight read* with some practice while the lock is installed. Sight reading involves manipulating the tumblers with a thin wire and noting the relative positions of each tumbler in the keyway. Since

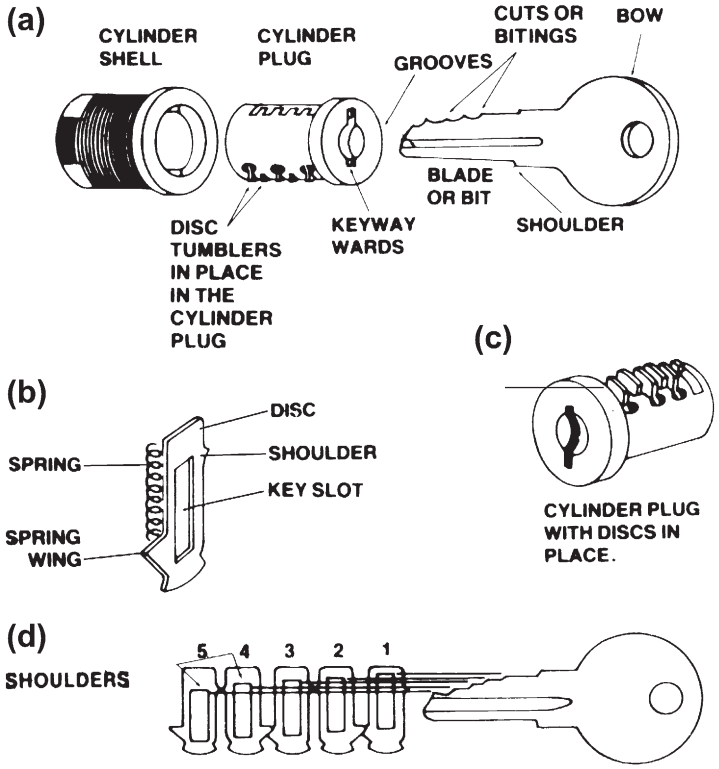


FIGURE 7-4 The key slots in the discs correspond to the cuts, or bitings, cut in the key. Note how each cut in the key will align its corresponding disc in a straight line with the others.

each lock has only a limited number of possible tumbler increments, the correct arrangement of these increments can be estimated with fair accuracy, permitting a key to be filed or cut on the spot to operate the lock.

Pin Tumbler Mechanisms

The pin tumbler mechanism is the most common type of key-operated mechanism used in architectural or builders' (door) hardware in the United States. The security afforded by this mechanism ranges from fair in certain inexpensive cylinders with wide tolerances and a minimum of tumblers to excellent with several makes of high-security cylinders, including those that are listed by Underwriters Laboratories (UL) as manipulation- and pick-resistant.

The lock operates very much like disc tumbler mechanisms (Figure 7-5). The locking system consists of a key, a cylinder plug, and a cylinder shell or housing. Rather than using discs, the mechanism uses pins as the basis interior barrier. Each lock contains an equal number of upper tumbler pins (drivers) and lower tumbler pins (key pins). The proper key has cuts or bitings to match the length of the lower pins. When it is inserted, the tops of the key pins are aligned flush with the top of the cylinder plug at the shear line. The plug may then rotate to lock or unlock the mechanism. When the key is withdrawn, the drivers are pushed by springs into the cylinder plus, pushing the key pins ahead of them until the key pins are seated at the bottom of the pin chamber. The drivers extending into the plug prevent it from rotating (Figure 7-6).

If an improper key is inserted, at least one key pin will be pushed into the shell, or one driver will extend into the plug. In either case, the pin extending past the shear line binds the plug to

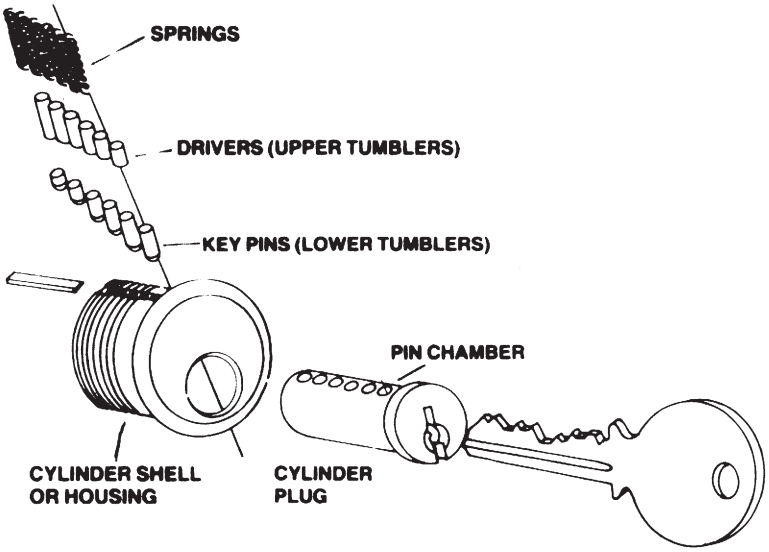


FIGURE 7-5 Basic pin tumbler cylinder lock mechanism.

the shell. One or more key pins may be aligned at the shear line by an incorrect key, but all will be aligned only when the proper key is used.

Depth intervals commonly used for pin tumbler cylinders vary from 0.0125 to 0.020 inches. These intervals allow between 5 and 10 depths for each tumbler position. The number of pins used ranges from three to eight—five or six is the most common number. Maximum useful combinations for most standard pin tumbler cylinders (assuming eight tumbler depth increments) are as follows:

Three pin tumblers, approximately 130 combinations
Four pin tumblers, approximately 1,025 combinations
Five pin tumblers, approximately 8,200 combinations
Six pin tumblers, approximately 65,500 combinations

These estimates assume that the useful combinations amount to no more than 23% of the mathematically possible combinations. Many common pin tumbler locks use fewer than eight increments, so the number of useful combinations for a specific lock may be much lower than the figures given in the table. Master keying will also greatly reduce the number of useful combinations.

Pin tumbler mechanisms vary greatly in their resistance to manipulation. Poorly constructed, inexpensive cylinders with wide tolerances, a minimum number of pins, and poor pin chamber alignment may be manipulated quickly by persons of limited ability. Precision-made cylinders with close tolerances, a maximum number of pins, and accurate pin chamber alignment may resist picking attempts even by experts for a considerable time.

Most pin tumbler lock mechanisms use warded keyways for additional security against incorrect keys and manipulation. The wards projecting into the keyway must correspond to grooves cut into the side of the key, or the key cannot enter the lock. When the wards on one side of the keyway extend past the center line of the key, and wards on the other side also extend past the center line; this is known as a *paracentric* keyway (Figure 7-7). While warded keyways are commonly used on most pin tumbler mechanisms, paracentric keyways are usually restricted to the better locks. They severely hinder the insertion of lockpicks into the mechanisms and the ability

of the manipulator to maneuver the pick once it is inserted.

Modifications have been made to the drives in better locks to provide increased security against picking (Figure 7-8). The usual modified shapes are the *mushroom* and the *spool*. Both of these shapes have a tendency to bind in the pin chamber when picking is attempted, making it more difficult to maneuver them to the shear line. To be consistently successful in picking pin tumbler cylinders with either type of modified driver, special techniques must be used.

There are a number of variations of the pin tumbler cylinder on the market. One, which is seeing increasingly widespread use, is the *removable core cylinder* (Figure 7-9). These locks were originally produced by the Best Universal Lock Company, whose initial patents have now expired. Most major architectural hardware manufacturers now have them available in their commercial lock lines. This type of cylinder uses a special key called the *control key* to remove the entire pin tumbler mechanism (called the *core*) from the shell. This makes it possible to quickly replace one core with another having a different combination and requiring a different key to operate. Because of this feature, removable core cylinders are becoming increasingly popular for institutional use and in large commercial enterprises where locks must be changed often.

Removable core cylinders do not provide more than moderate security. Most systems operate on

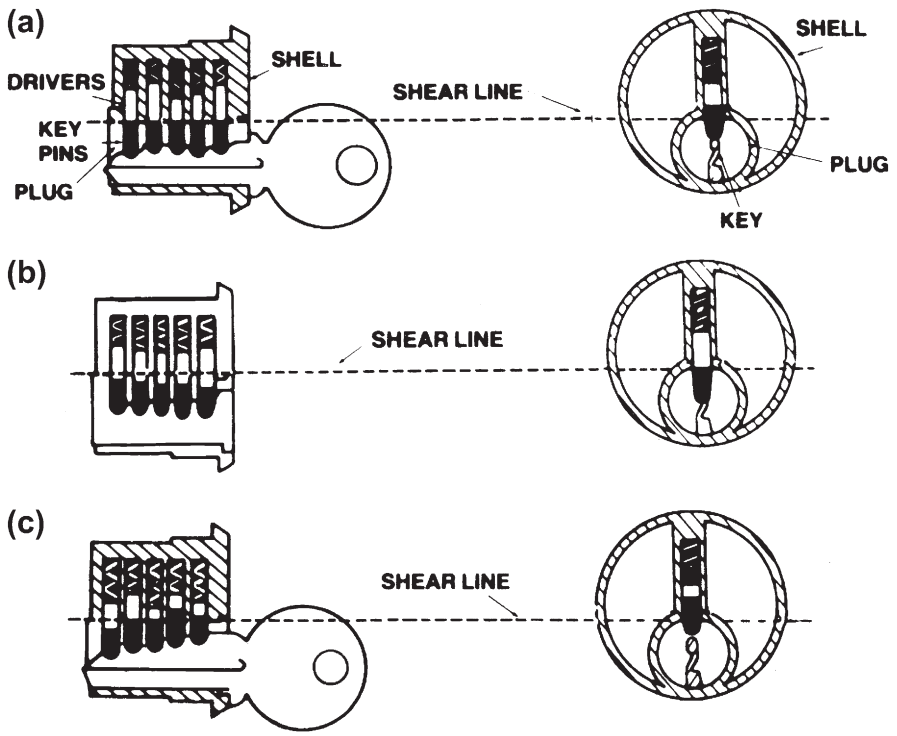


FIGURE 7-6 Operation of a pin tumbler cylinder mechanism: (a) When the correct key is inserted, the bitings in the key align the tops of the lower tumblers (key pins) with the top of the cylinder plug at the shear line. The plug may then be rotated in the shell to operate the lock. (b) When the key is withdrawn, the springs push the upper tumblers (drivers) into the cylinder plug. With the pins in this position, the plug obviously cannot be turned. (c) When an incorrect key is used, the bitings will not match the length of the key pins. The key will allow some of the drivers to extend into the plug, and some of the key pins will be pushed into the shell by high cuts. In either case, the plug cannot be rotated. With an improper key, some of the pins may align at the shear line, but only with the proper key will all five align so that the plug can turn.

a common control key, and possession of this key will allow entry through any lock in the system. It is not difficult to have an unauthorized duplicate of the control key made. If this is not possible, any lock, particularly a padlock, of the series may be borrowed and an unauthorized control key made. Once the core is removed from a lock, a screwdriver or other flat tool is all that is necessary to operate the mechanism. Additionally, the added control pins increase the number of shear points in each chamber, thus increasing the mechanism's vulnerability to manipulation.

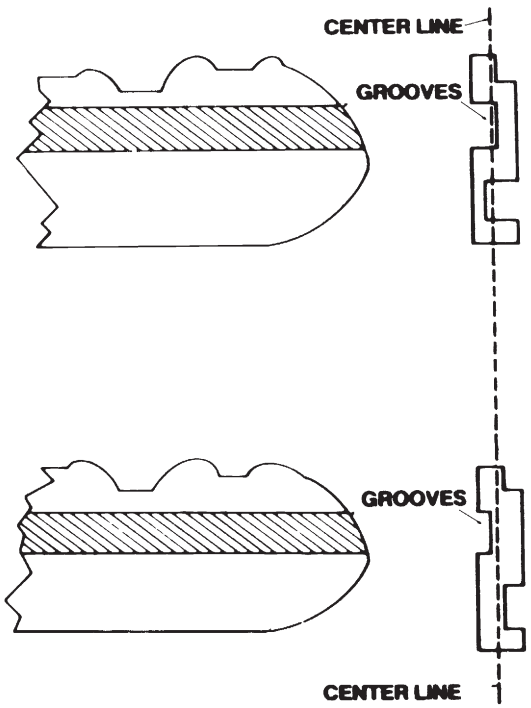


FIGURE 7-7 Milled, warded, and paracentric keys.

Another variation that has been in widespread use for many years is *master keying*. Almost any pin tumbler cylinder can easily be master-keyed. This involves the insertion of additional tumblers called *master pins* between the drivers and key pins. These master pins enable a second key, the *master key*, to operate the same lock (Figure 7-10). Generally, an entire series of locks is combinated to be operated by the same master key. There may also be levels of master keys, including submasters, which open a portion, but not all, of a series; master keys that open a larger part; and grand masters that open the entire series. In very involved installations, there may even be a fourth level (great grand master key).

There are a number of security problems with master keys. The most obvious one is that an unauthorized master key will permit access through any lock of the series. Less obvious is the fact that master keying reduces the number of useful combinations that can be employed since any combination used must not only be compatible with the change key, but with the second, master key. If a submaster is used in the series, the number of combinations is further reduced to those which are compatible with all three keys. If four levels of master keys are used, it should be obvious that the number of useful combinations becomes extremely small. If a large number of locks are involved, the number of locks may exceed the number of available combinations. When this occurs, it may be necessary to use the

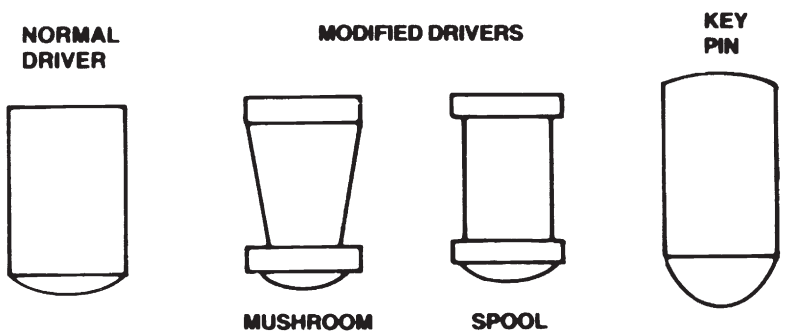


FIGURE 7-8 Pin tumbler modification.

same combination in several locks, which permits one change key to operate more than one lock (*cross keying*). This creates an additional security hazard.

One way of increasing the number of usable combinations and decreasing the risk of cross keying is to use a *master sleeve* or ring. This sleeve fits around the plug, providing an additional shear line similar to the slide shear line in a removable core system. Some of the keys can be cut to lift tumblers to sleeve shear line, and some to the plug shear line. This system, however, requires the use of more master pins. Any increase in master pins raises the susceptibility of the lock to manipulation, since the master pins create more than one shear point in each pin chamber, increasing the facility with which the lock can be picked.

Thus, while master-keyed and removable-core systems are necessary for a number of very practical reasons, you should be aware that they create additional security problems of their own.

The basic pin tumbler mechanism has been extensively modified by a number of manufacturers to improve its security. The common features of high-security pin tumbler cylinder mechanisms are that they are produced with extremely close tolerances and that they provide a very high

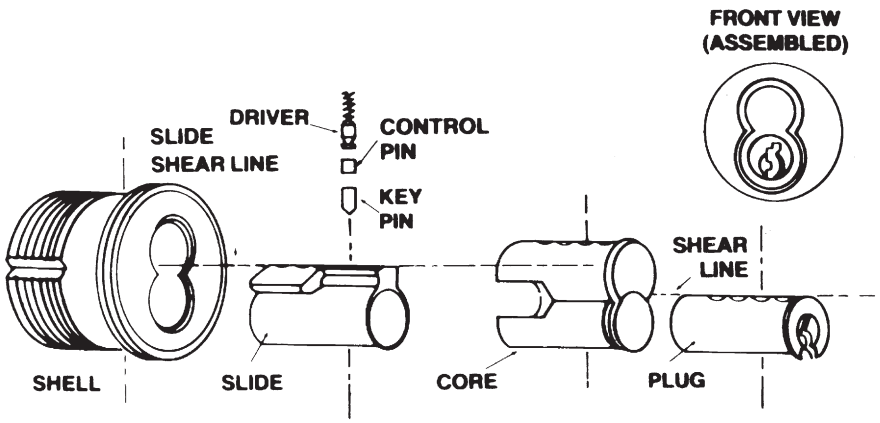


FIGURE 7-9 Removable core, pin tumbler, cylinder mechanism.

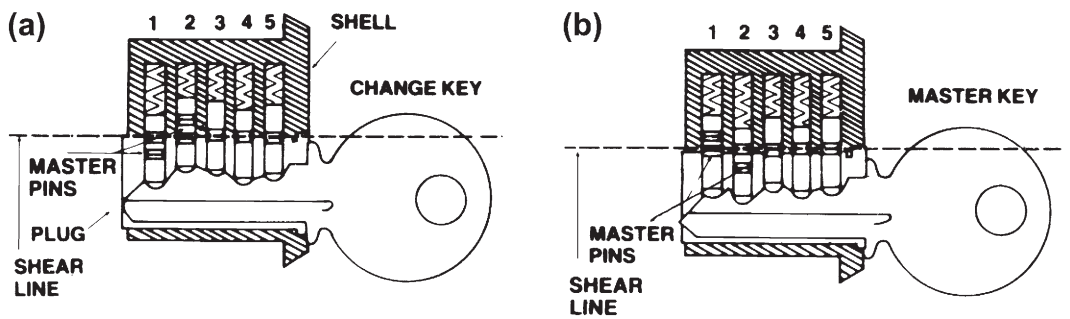


FIGURE 7-10 Master-keyed pin tumbler cylinder mechanism: (a) This is a simple master-keyed system using master pins in the first and second tumbler positions. When the change key is inserted, note that the top of the first master pin aligns with the top of the cylinder plug. The remaining positions show the key pins aligned with the top of the plug. This arrangement permits the plug to turn. (b) With the master key inserted, the first position aligns the top of the key pin with the cylinder plug. The master pin is pushed farther up the pin cylinder. The second position shows the master pin aligning at the top of the plug. The master pin has dropped farther down the pin hole in the plug. The remaining three positions are unchanged. This arrangement also allows the plug to rotate.

number of usable combinations. Additional security features include the use of very hard metals in their construction to frustrate attacks by drilling and punching.

Lever Tumbler Mechanisms

Although the lever lock operates on the same principles as the pin or disc tumbler mechanism, its appearance is very different. Figure 7-11 illustrates a typical lever mechanism. Unlike pin or disc tumbler devices, the lever lock does not use a rotating core or plug, and the bolt is usually an integral part of the basic mechanism thrown directly by the key. The only other type of mechanism in which the key directly engages the bolt is the warded mechanism. You will recall that the bolt in pin or disc tumbler systems is usually directly operated by the *cylinder plug*, not the key. The key is used to rotate the plug, but never comes into direct contact with the bolt.

Despite these somewhat deceptive appearances, the lever lock operates very much like the other tumbler mechanisms. Each *lever* is hinged

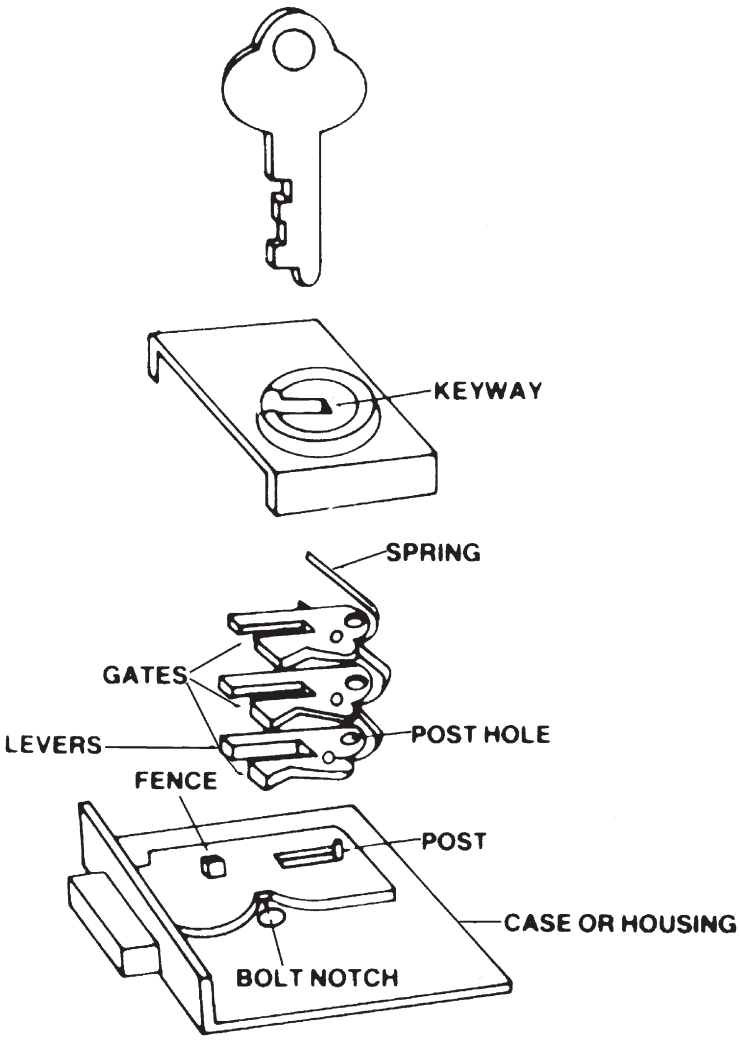


FIGURE 7-11 Lever tumbler mechanism.

on one side by the *post*, which is a fixed part of the case. The *leaf springs* attached to the levers hold them down in a position that overlaps the *bolt notch* as shown in Figure 7-12. In this position, the *bolt* is prevented from moving back into a retracted position by its *fence*, which is trapped by the front edges (*shoulder*) of the levers. When the key is inserted and slightly rotated, the bitings

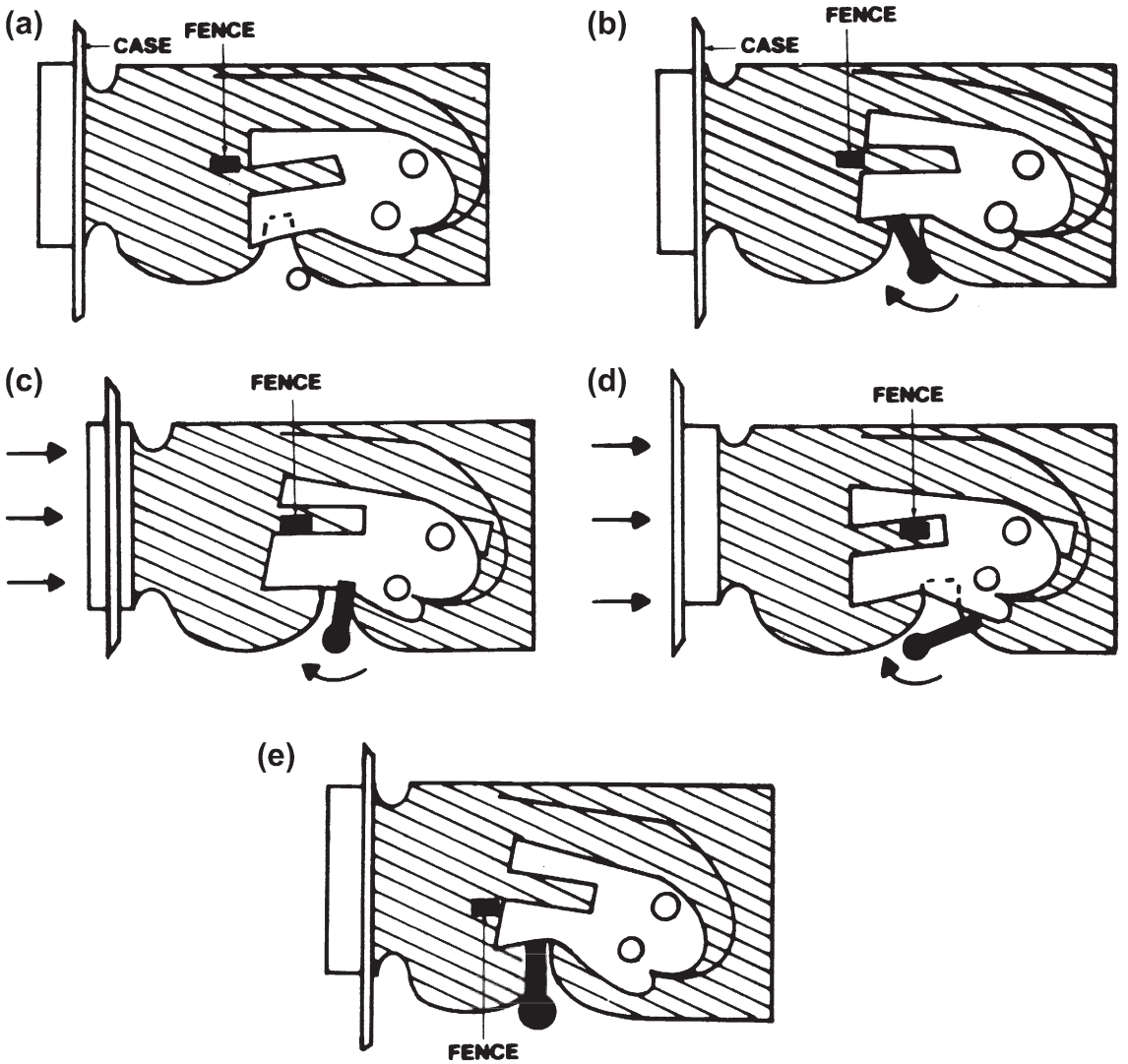


FIGURE 7-12 Operation of a typical lever tumbler mechanism: (a) The bolt is in the fully extended locked position and the key has been withdrawn from the keyway. In this position, the spring forces the lever down toward the bolt notch, trapping the fence against the forward edge (shoulder) of the lever. This prevents the bolt from being forced back. (b) The key has been inserted and the biting on the key has lifted the lever against the spring tension, aligning the gate with the fence. The bolt can now be moved back into the retracted position. (c) The key has begun to force the bolt back into a retracted position by engaging a shoulder of the bolt notch at the same time it is keeping the lever suspended at the correct height to allow the fence to pass into the gate. (d) The bolt is now fully retracted and the key can be withdrawn. (e) If an improper key is inserted the biting either will not lift the lever high enough for the fence to pass through the gate or the lever will be raised too high and the fence will be trapped in front of the lower forward shoulder of the lever. From this position, the bolt cannot be forced back into the retracted position.

on the key engage the *saddle* of the lever, raising it to a position where the fence aligns with the slot in the lever (called the *gate*). In this position, the fence no longer obstructs the movement of the bolt to the rear, and the bolt can be retracted.

The retraction is accomplished by the key engaging the shoulder of the bolt notch. While the bitings of the key are still holding the levers in an aligned position, the key contacts the rear shoulder of the bolt notch, forcing the bolt to retract as the key is rotated. As the bolt is retracted, the fence moves along the gate until the bolt is fully withdrawn. When the key has rotated fully, completely retracting the bolt, it can be withdrawn.

If an improperly cut key is inserted and rotated in the lock, either the levers will not be raised far enough to align all of the gates with the fence, or one or more levers will be raised too high, so that the bottom edge of the lever obstructs the fence (as in Figure 7-12). In either case, the bolt is prevented from being forced to the rear, thus opening the lock.

Figure 7-13(a) shows one version of the basic lever. A number of variations are on the market. Some levers are made with projections built into the gate designed to trap the fence in various positions (Figure 7-13b). The front and rear traps prevent the fence from being forced through the gate when the bolt is in the fully extended or fully retracted position. Figure 7-13(c) shows another variation: serrated (saw-tooth) front edges. These serrations are designed to bind against the fence when an attempt is made to pick the lock. They are commonly found on high-security lever tumbler mechanisms.

Lever mechanisms provide moderate to high security depending on the number of levers used, their configuration, and the degree of care used in the construction of the lock mechanism. Any mechanisms using six or more tumblers can

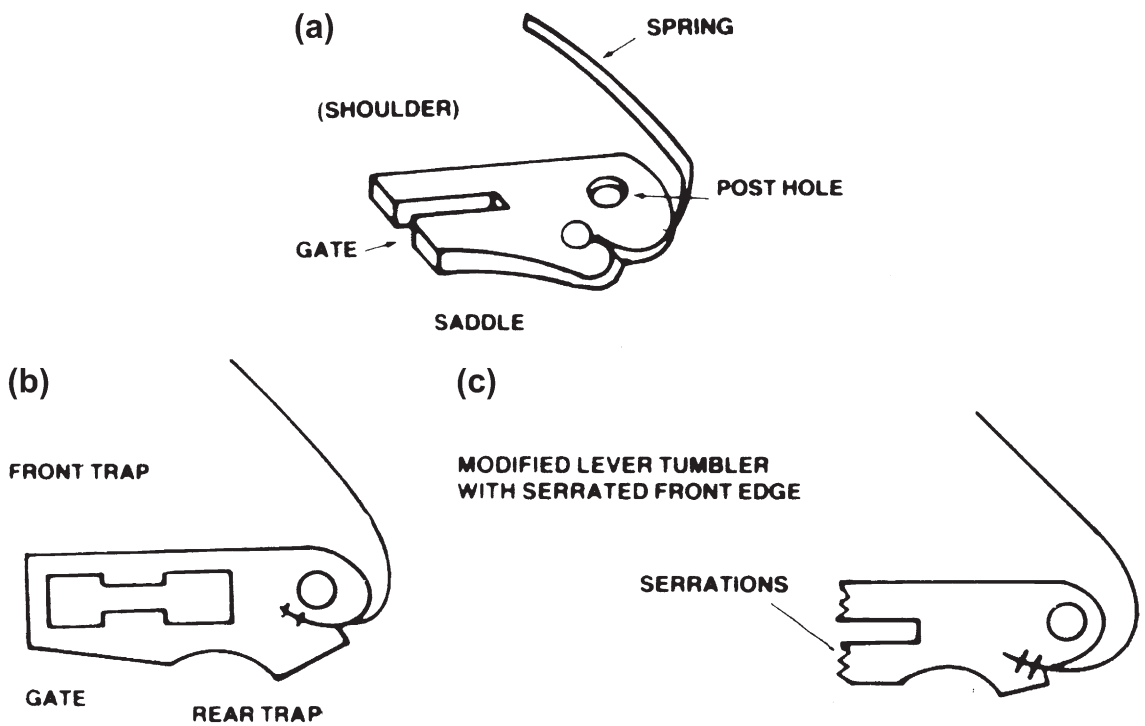


FIGURE 7-13 Lever tumblers. To operate the lock, the key contacts the lever at the saddle, lifting it until the fence is aligned with the gate. The saddles on the various tumblers are milled to different depths to correspond to different cuts on the key.

safely be considered a high-security lock. Some mechanisms use a double set of levers, requiring a double-bited key. The levers are located on both sides of the keyway. This configuration makes the lock very difficult to pick or manipulate.

Lever locks are commonly found in applications where moderate to high security is a requirement, including safe deposit boxes, strong boxes, post office boxes, and lockers. The lever mechanisms available in the United States, because of the integrated, short-throw bolt, are not ordinarily used as builders' hardware. But they are commonly used in that application in Europe, and some of these locks have found their way into the United States.

COMBINATION LOCKS

In principle, a combination lock works in much the same way as a lever mechanism. When the tumblers are aligned, the slots in the tumblers permit a fence to retract, which releases the bolt so that the bolt can be opened. The difference is that where the lever mechanism uses a key to align the tumblers, the combination mechanism uses numbers, letters, or other symbols as reference points that enable an operator to align them manually. Figure 7-14 shows a simplified view of a typical three-tumbler combination lock mechanism. The tumblers are usually called *wheels*. Each wheel has a slot milled into its edge, which is designed to engage the *fence* when the slot has been properly aligned. This slot is called a *gate*. The fence is part of the lever that retracts the bolt. The gates are aligned with the fence by referring to letters, numbers, or other symbols on the dial. The sequence of symbols that permits the lock to operate is its *combination*. A typical combination sequence using numbers is 10–35–75. The fact that three numbers are used in the combination indicates that the lock contains three tumblers. The number of tumblers in a lock always corresponds to the number of symbols used in its combination. Few modern combination locks use more than four tumblers because combinations of five or more symbols are unwieldy and hard to remember. Older models, however, used as many as six.

Both *drive cam* and dial are fixed to the *spindle* so that as the dial is rotated, the drive cam will also rotate in an identical fashion. The drive

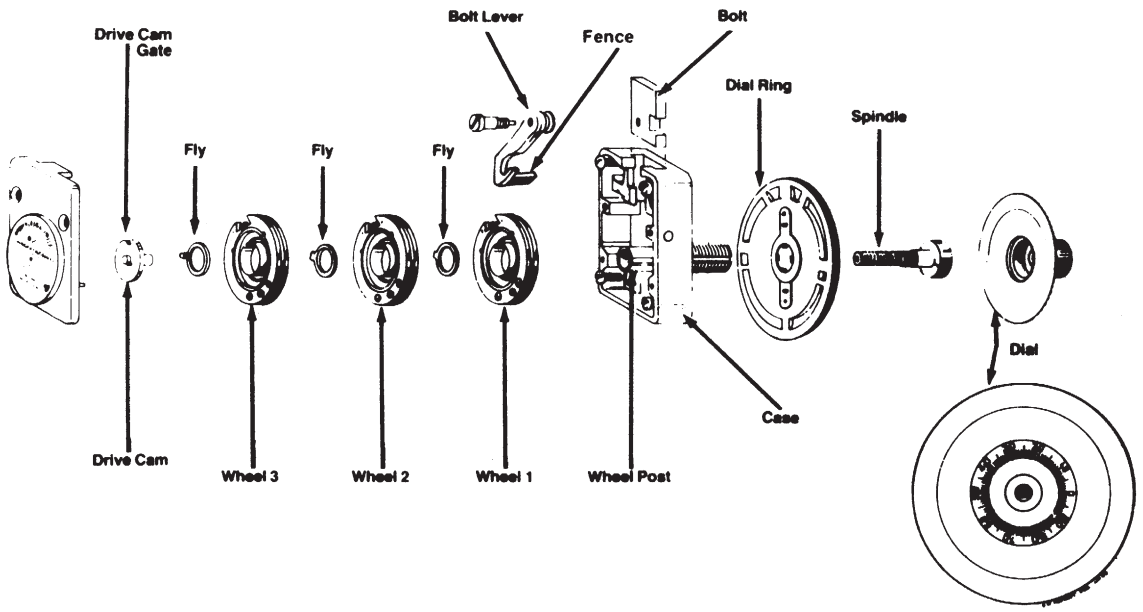


FIGURE 7-14 Three-tumbler combination.

cam has two functions. It is the means by which motion of the dial is transferred to the wheels, and when all wheels are properly aligned and the fence retracted, it is the mechanism by which the bolt lever is pulled to retract the bolt.

The wheels are not fixed to the spindle, but ride on a *wheel post* that fits over the spindle. These wheels are free-floating and will not rotate when the dial is turned unless the *flies* are engaged. The flies are designed to engage pins on the wheels at predetermined points (determined by the combination of that particular lock). When the flies engage these pins, the wheels pick up the rotating motion of the dial. When the flies are not engaged, the wheels will remain in place when the dial is rotated.

To operate a typical three-wheel combination lock, the dial is first turned four times in one direction to allow all of the flies to engage their respective wheels so that as the dial is being turned, all of the wheels are rotating with it. At this point the wheels are said to be *nested*. The object is to disengage each wheel at the spot where its gate will be aligned with the fence. To do this, the operator stops the dial when the first number of the combination reaches the index mark on the dial ring. This first stop aligns the gate of wheel 1 with the fence.

The operator then reverses direction to disengage wheel 1, which remains stationary, and rotates the dial three turns to the second number in the combination. When this number is under the index mark, wheel 2 is aligned. Again reversing direction to disengage wheel 2, the operator makes two turns to the last number of the combination. This aligns wheel 3. At this point all of the gates are aligned with the fence. The operator then reverses direction once again and turns the dial until it stops.

This last operation has two functions. It aligns the gate on the drive cam with the fence, which permits the fence to retract into the space provided by the three gates in the wheels and the fourth gate in the drive cam. The bolt lever is now engaged with the wheels and drive cam. As the operator continues rotating the dial, the drive cam pulls the bolt lever to retract the bolt. When the dial will no longer rotate, the bolt is fully retracted, and the lock is open.

The security afforded by combination mechanisms varies widely. The critical elements are the number of tumblers used in the lock, the number of positions on the tumbler where the gate can be located, and the tolerances in the width of the gate and fence. Wide tolerances allow the fence to enter the gates even when they are not quite completely aligned, so that, although the proper combination may be 10–35–75, the lock may also operate at 11–37–77.

Until the 1940s it was often possible to open many combination locks by using the sound of the movement of the tumblers and feeling the friction of the fence moving over the tumblers as indicators of tumbler position. (Tumblers in combination locks do not click despite Hollywood's contentions to the contrary.) Skilled operators were often able to use sound and feel to determine when each tumbler came into alignment. Modern technology has all but eliminated these possibilities, however, through the introduction of sound baffling devices, nylon tumblers, improved lubricants to eliminate friction, false fences, and cams that suspend the fence over the tumblers so that they do not make contact until after the gates are already aligned (see Figure 7-14).

Another manipulation technique of recent vintage utilized the fact that the tumbler wheels with gates cut into them are unbalanced: more weight is on the uncut side than on the cut side. By oscillating the dial, these cut and uncut sides could be determined, and the location of the gates estimated. The introduction of counterbalanced tumblers has virtually eliminated this approach to the better mechanisms.

Radiology has also been used to defeat combination locks. A piece of radioactive material placed near the lock can produce ghost images of the tumblers on sensitive plates, showing the location of the gates. Nylon and Teflon tumblers and shielding material that are opaque to radiation are used to defeat this technique.

LOCK BODIES

Most lever tumbler and warded mechanisms contain an integrated bolt as a part of the

mechanism. The key operates directly to throw the bolt, thereby opening and locking the lock. This is not true of pin and disc tumbler locks. These consist of two major components. The cylinder plug, the shell, the tumblers, and springs are contained in an assembly known as the *cylinder*. The other major component is the *lock body*, which consists of the *bolt assembly* and case or housing. The bolt assembly consists of the bolt, a *rollback*, and a *refractor*. This assembly translates the rotating motion of the cylinder plug to the back-and-forth motion that actually operates the bolt. When the cylinder is inserted into the lock body, it is typically connected to the bolt assembly by a *tail piece* or cam. A cylinder can be used in a number of different lock bodies. Here we will be primarily concerned with the types of bodies used on standard residential and light commercial doors. The pin tumbler is the usual mechanism used in these locks, although some manufacturers offer door locks using disc tumbler cylinders (such as the Schlage Cylindrical Lock).

Bolts

There are two types of bolts used for most door applications: the *latch bolt* and the *dead bolt*. Examples of these are illustrated in Figure 7-15. They are easily distinguished from each other. A latch bolt always has a beveled face, while the face on a standard dead bolt is square.

Latch Bolt. This bolt, which is sometimes called simply a latch, a locking latch (to distinguish it from nonlocking latches), or a spring bolt is always spring-loaded. When the door on which it is mounted is in the process of closing, the latch bolt is designed to automatically retract when its beveled face contacts the lip of the strike. Once the door is fully closed, the latch springs back to extend into the hole of the strike, securing the door.

A latch bolt has the single advantage of convenience. A door equipped with a locking latch will automatically lock when it is closed. No additional effort with a key is required. It does not, however, provide very much security.

The throw on a latch bolt is usually ⅜ inch but seldom more than ⅝ inch. Because it must be able to retract into the door on contact with the lip of the strike, it is difficult to make the throw much longer. But, because there is always some space between the door and the frame, this means that a latch may project into the strike no more than ¼ inch (often as little as ⅛ inch on poorly hung doors). Most door jambs can be spread at least ½ inch with little effort, permitting an intruder to quickly circumvent the lock.

Another undesirable feature of the latch bolt is that it can easily be forced back by any thin shim (such as a plastic credit card or thin knife) inserted between the face plate of the lock and the strike. Antishim devices have been added to the basic latch bolt to defeat this type of attack. They are designed to prevent the latch bolt from being depressed once the door is closed. Figure 7-16(a) shows a latch bolt with antishim device. These are often called *deadlocking*

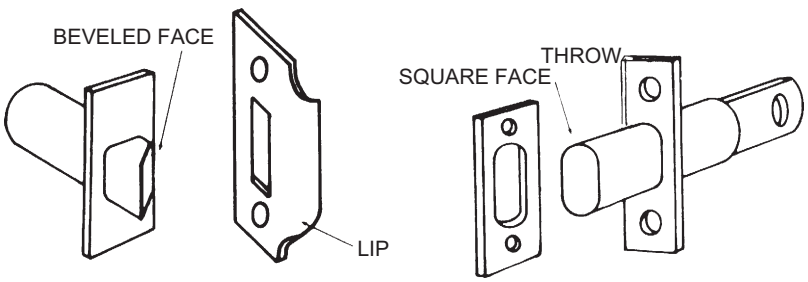


FIGURE 7-15 Basic types of bolts.

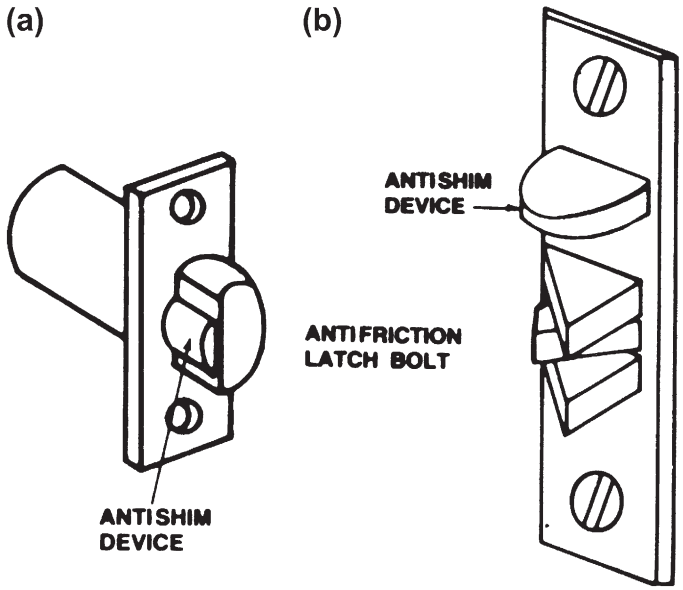


FIGURE 7-16 Modified latch bolts: (a) latch bolt with antishim device, and (b) antifriction latch bolt with antishim device.

latches, a term that is mildly deceptive since these latches do not actually deadlock and they are not nearly as resistant to jimmying as deadlocks. Often a thin screwdriver blade can be inserted between the face plate and the strike and pressure applied to break the antishim mechanism and force the latch to retract.

Another type of latch bolt, shown in Figure 7-16(b), is called an *antifriction latch bolt*. The antifriction device is designed to reeclosing pressure required to force the latch bolt to retract. This permits a heavier spring to be used in the mechanism. Most modern antifriction latches also incorporate an antishim device. Without it, the antifriction latch is extremely simple to shim.

Dead Bolt. The dead bolt is a square-faced solid bolt that is not spring-loaded and must be turned by hand into the locked and unlocked position. When a dead bolt is incorporated into a locking mechanism, the result is usually known as *deadlock*. The throw on a standard dead bolt is also about ½ inch, which provides only minimal protection against jamb spreading. A *long-throw dead bolt*, however, has a throw of 1 inch or longer. One inch is considered the minimum for adequate protection. Properly installed in a good door using a secure strike, this bolt provides reasonably good protection against efforts to spread or peel the jamb.

The ordinary dead bolt is thrown horizontally. On some narrow-stile doors, such as aluminum-framed glass doors, the space provided for the lock is too narrow to permit a long horizontal throw. The *pivoting dead bolt* is used in this situation to get the needed longer throw (Figure 7-17a). The pivoting movement of the bolt allows it to project deeply into the frame, at least 1 inch, usually more. A minimum of 1 inch is recommended. When used with a reinforced strike, this bolt can provide good protection against efforts to spread or peel the frame.

Increased security against jamb spreading is provided by a number of different types of dead bolts that collectively are known as *interlocking dead bolts*. These are specifically designed to interlock the door and the strike so that the door jamb cannot be spread. The most common of these is the *vertical-throw dead bolt* shown in Figure 7-17(b). This is usually a rim-mounted device. The other two devices shown in Figure 7-17(c–d) (the *expanding bolt dead bolt* and the *rotating dead bolt*) are meant to be mounted

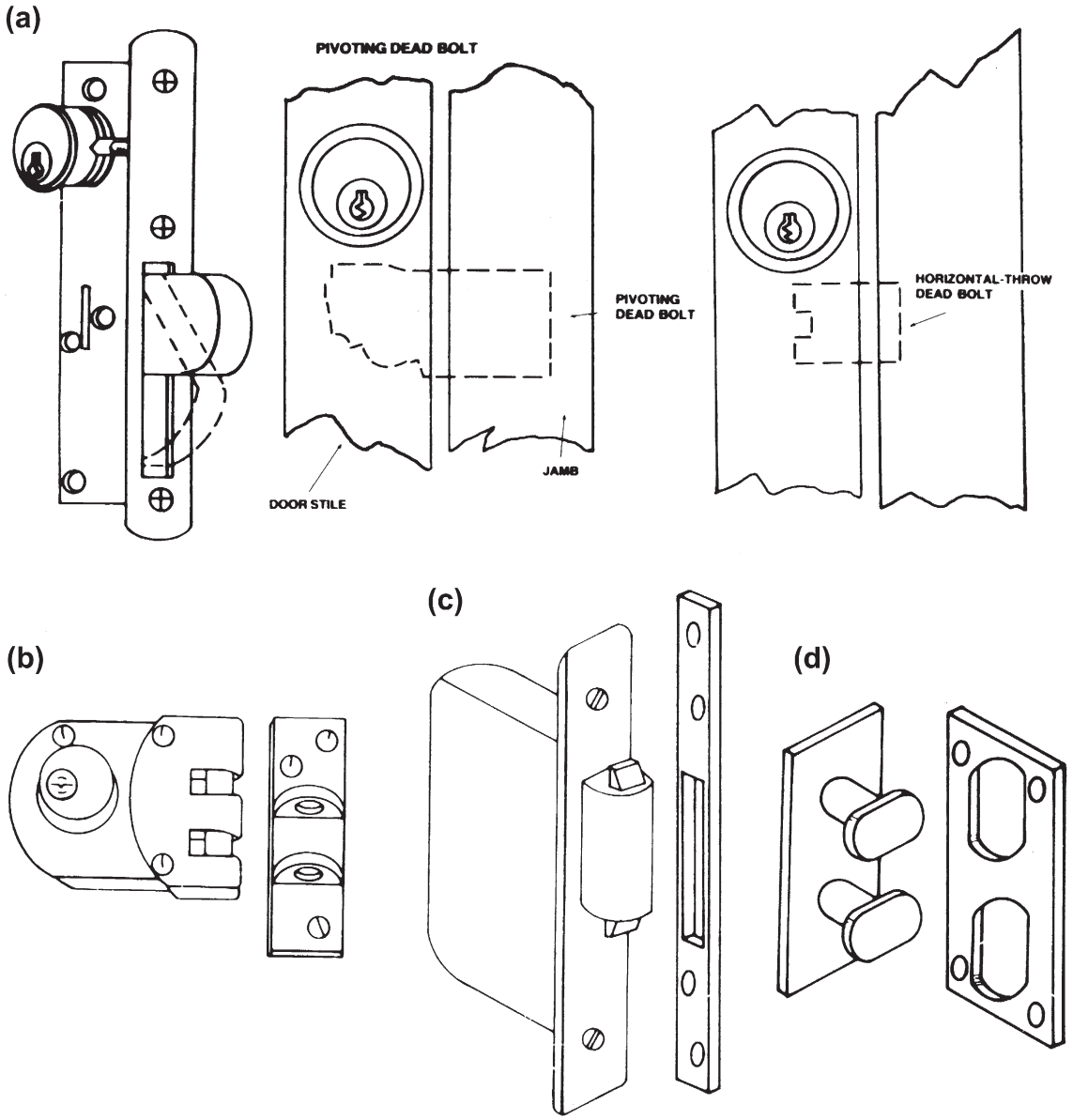


FIGURE 7-17 Modified dead bolts. Note the difference in penetration into the jamb. The deeper penetration afforded by the pivoting bolt increases protection against jamb spreading.

inside the door. These locks require a securely mounted strike or they are rendered ineffective.

DOOR LOCK TYPES

Five basic lock types are used on most doors in the United States: mortise, rim-mounted, tubular, cylindrical, and unit. Each of these has a number of advantages and disadvantages from the point of view of the protection offered. Each, however, with the single exception of the cylindrical lockset, can offer sound security when a good lock is properly installed.

Mortise

It was but a few years ago that almost all residential and light commercial locks were mortise locks. A mortise lock, or lockset, is installed by hollowing out a portion of the door along the front or leading edge and inserting the mechanism into this cavity. Suitable holes are then drilled into the side of the door in the appropriate spot for the cylinders and door knob spindle (where the door knob is part of the unit, as is usually the case). Figure 7-18(a) shows a typical mortise lockset. These mechanisms require a door that is thick enough to be hollowed out without losing a great deal of its strength in the process. One of the major weaknesses of mortise locks is that the cylinder is usually held in the lock with a set screw, which provides very little defense against pulling or twisting the cylinder out of the lock with a suitable tool. Cylinder guard plates can be used to strengthen the lock's resistance to this threat. On some mortise locks, the trim plate acts as a cylinder guard.

Rim-Mounted

A rim-mounted mechanism is simply a lock that is installed on the surface (rim) of the door (Figure 7-18b). Most are used on the inside surface, since outside installation requires a lock that is reinforced against direct attacks on the case. These are usually supplementary locks installed where the primary lock is not considered enough protection. These may or may not be designed for key operation from the outside. If they are, a cylinder extends through the door to the outside where it can be reached by a key.

Tubular

This lock (sometimes called a bore-in) is installed by drilling a hole through the door to accommodate the cylinder (or cylinders) and a hole drilled from the front edge of the door to the cylinder for the bolt assembly (Figure 7-18c). This type of installation has virtually replaced the mortise lock in most residential and light commercial applications because it can be installed quickly and by persons of limited skill.

Cylindrical Lockset

The cylindrical lockset ordinarily uses a locking latch as its sole fastening element (Figure 7-18d). It is installed like the tubular lock by drilling two holes in the door. The cylinders are mounted in the doorknobs, rather than in a case or inside the door, which makes them vulnerable to just about any attack (hammering, wrenching, etc.) that can knock or twist the knob off the door. Unfortunately, because it is inexpensive and simple to install, about 85% of all residential locks currently used in new construction in the United States are of this type. It provides virtually no security whatsoever. There is perhaps no harder or faster rule in lock security than the rule that all cylindrical locks should be supplemented by a secure, long-throw dead bolt. Or, better yet, they should be replaced. A number of more secure locks designed to replace the cylindrical lock are now on the market. One of these is illustrated in Figure 7-18d.

Unit Locks

A unit lock is installed by making a U-shaped cutout in the front edge of the door and slipping the lock into this cutout (Figure 7-18e). This type of lock usually has the advantage of having no exposed screws or bolts. It is ordinarily used in place of mortise locks where the door is too narrow to mortise without considerable loss of strength. A good unit lock properly installed on a solid door provides excellent protection against attempts to remove the cylinder, or to pry or twist the lock off the doors.

Cylinders

Cylinders are mounted in the lock body in a number of ways. Most mortise cylinders are threaded into the lock and secured with a small set screw (Figure 7-19). Tubular and rim locks use cylinder

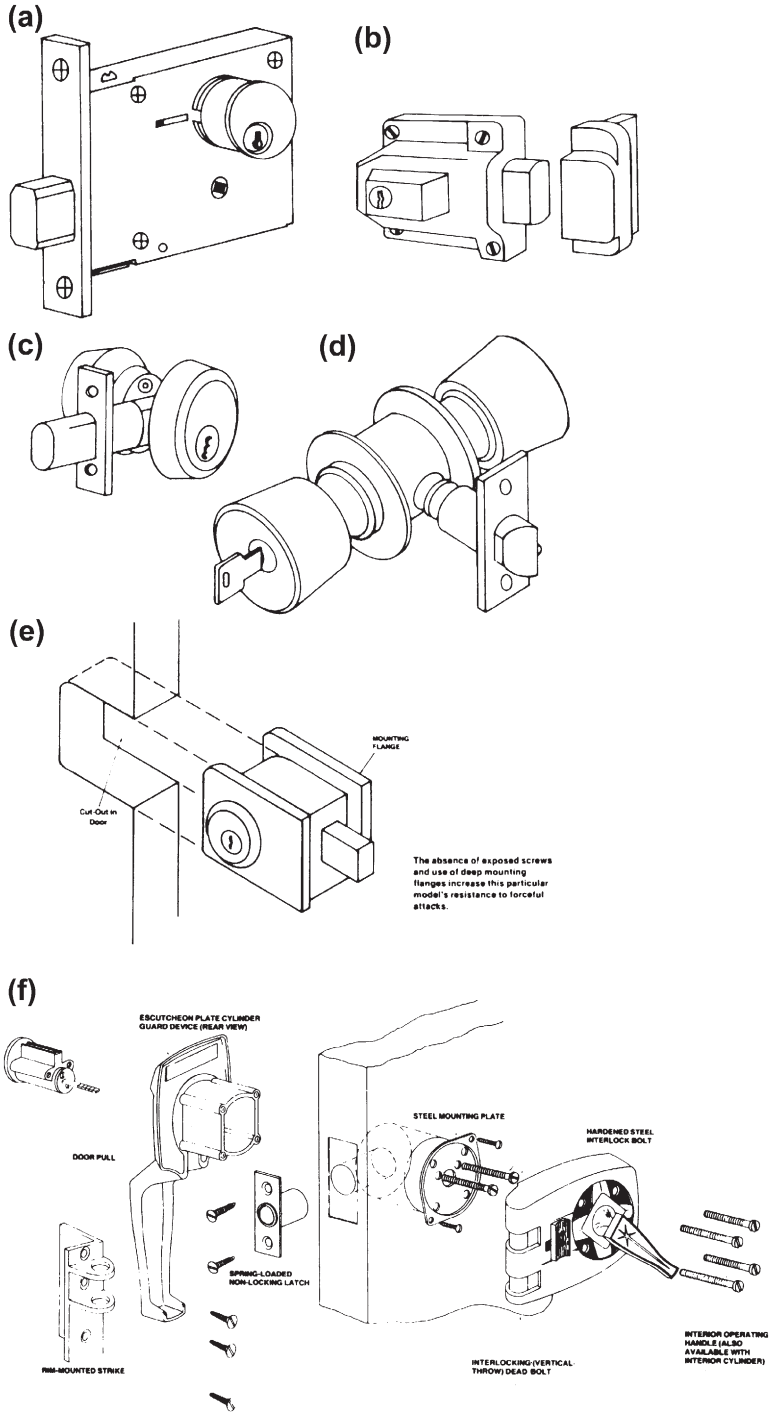


FIGURE 7-18 Lock types: (a) mortise deadlock, (b) rim deadlock with rim strike, (c) tubular deadlock, (d) cylindrical (lock-in-knob) lockset, (e) unit lock, (f) Ideal Superguard Lock II. Note washers must be used for additional protection against cylinder pulling. These are not supplied with the lock.

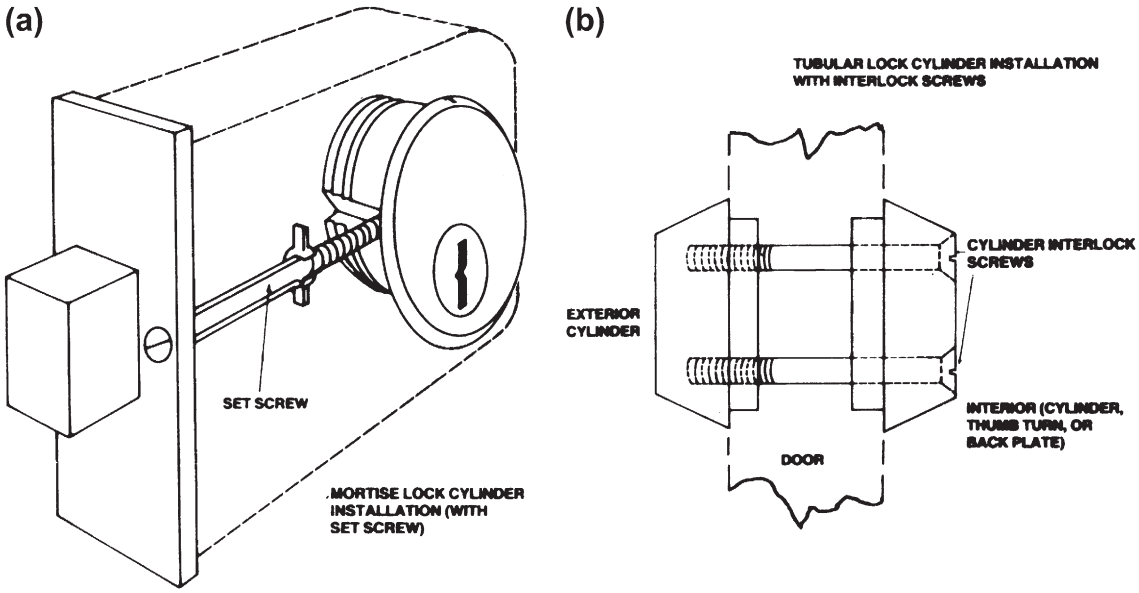


FIGURE 7-19 Mortise lock cylinder installation: (a) with set screw, and (b) with interlock screws.

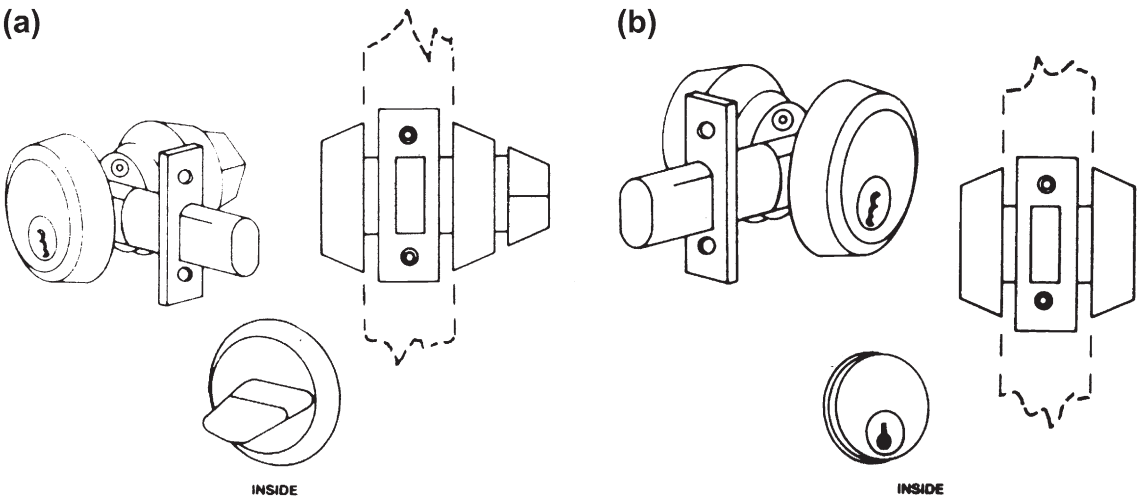


FIGURE 7-20 (a) Single cylinder deadlock with interior thumb turn. (b) Double cylinder deadlock with interior key cylinder.

interlock screws inserted from the back of the lock. Better mechanisms use ¼-inch or larger diameter hardened steel screws for maximum resistance to pulling and wrenching attacks (Figure 7-19). Better cylinders incorporate hardened inserts to resist drilling.

Two basic cylinder configurations are available. *Single cylinder* locks use a key-operated cylinder on the outside, and a thumb-turn or blank plate on the inside (Figure 7-20). *Double cylinder* locks use a key-operated cylinder on both sides of the door (Figure 7-20). This prevents an intruder from breaking a window near the door, or punching a hole through the door, reaching in, and turning the lock from the inside. The disadvantage of double cylinders is that

rapid exit is made difficult since the key must first be located to operate the inside cylinder. If a fire or other emergency makes rapid evacuation necessary, a double cylinder lock could pose a considerable hazard.

Padlocks

The distinguishing feature of padlocks is that they use a shackle rather than a bolt as the device that fastens two or more objects together (Figure 7-21). The shackle is placed through a hasp, which is permanently affixed to the items to be fastened. Three methods are commonly used to secure the shackle inside the lock body. The simplest and least secure method is to press a piece of flat spring steel against an indentation in the shackle. When the key is inserted, it rotates to spread the spring releasing the shackle (Figure 7-22). This is a locking method commonly found on warded padlocks. It is found more rarely on tumbler-type locks, but it is found occasionally on the less expensive models.

A slightly more secure method uses a locking dog. The dog is spring-loaded and fits into a notch cut into the shackle (Figure 7-22). The key is used to retract the dog, permitting the shackle to be withdrawn. Both of these spring-loaded

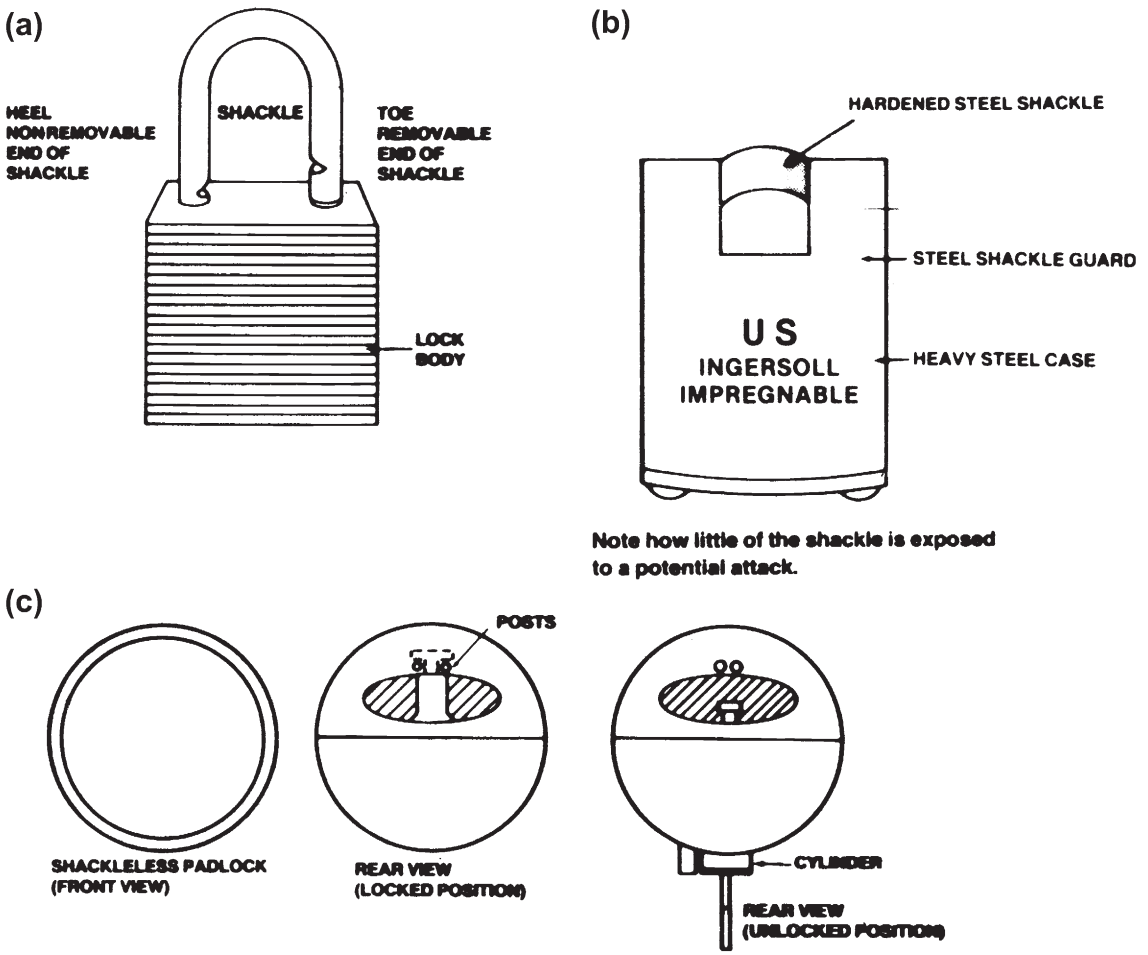


FIGURE 7-21 (a) Warded padlock. (b) High-security padlock. (c) Shackleless padlock.

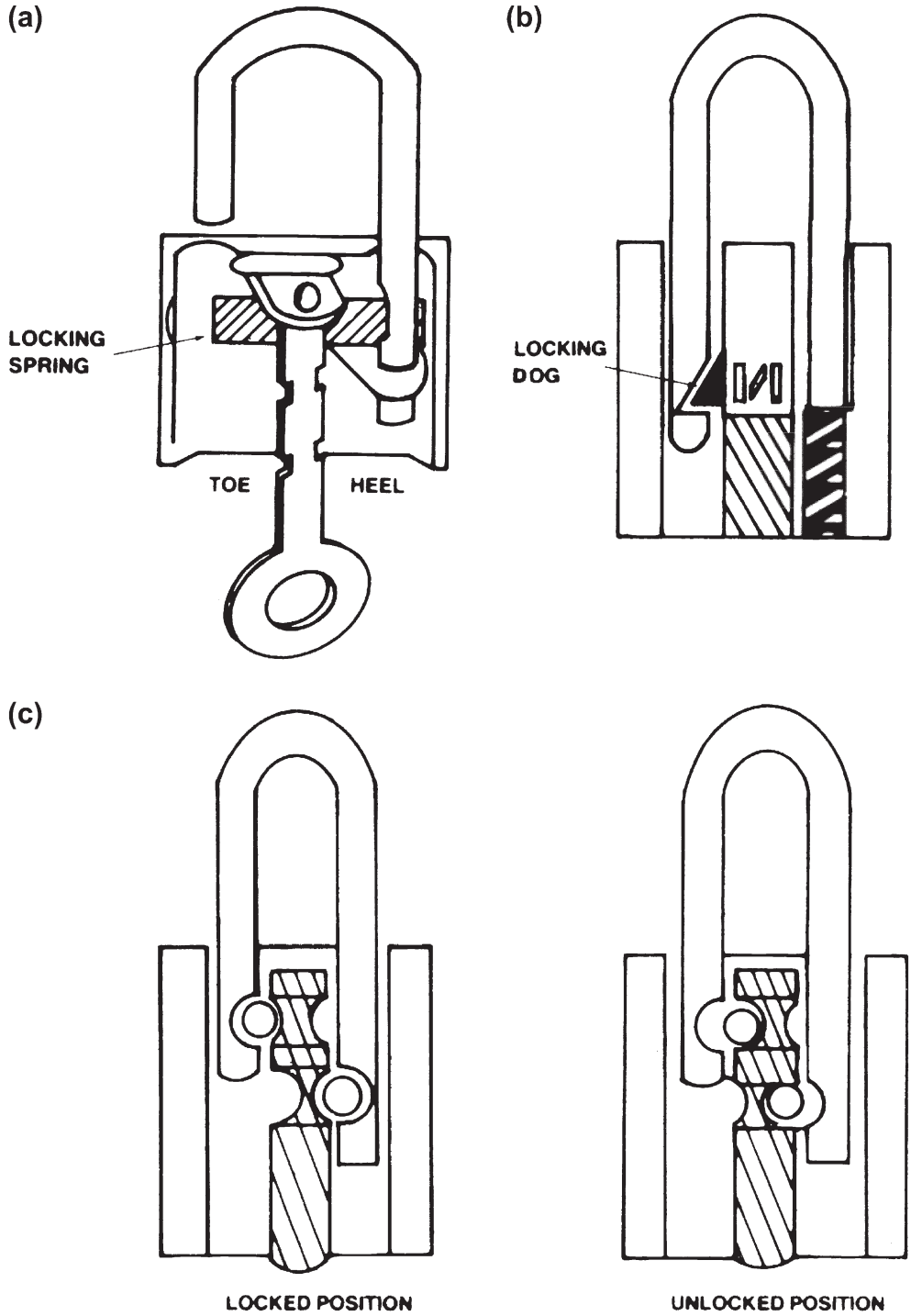


FIGURE 7-22 Three methods of securing the shackle inside the lock body: (a) warded padlock with locking spring (heel locking), (b) padlock with locking dog (toe locking), and (c) positive locking padlock (heel and toe locking).

mechanisms are vulnerable to attacks that take advantage of the fact that the locking device can be forced back against the spring by a suitable tool. Shimming and rapping are common techniques used to open them. Often a stiff wire can be pushed down the shackle hole to engage and force back the spring or locking dog. Spring-loaded padlocks should not be used where reasonable security is required.

Positive locking techniques do much to reduce the vulnerability of padlocks to these types of attacks. The most common positive locking method uses steel balls inserted between the cylinder and the shackle. In the locked position, the ball rests half in a groove in the cylinder, and half in a notch cut into the shackle. In this position the shackle cannot be forced past the steel ball. When the cylinder is turned to the unlocked position, the groove deepens, permitting the ball to retract into the cylinder when pressure is put on the shackle. This releases the shackle and opens the lock. These locks are designed so that the key cannot be removed unless the lock is in the locked position.

Padlocks are vulnerable to attacks at several points. The shackle can be pried out of the lock by a crowbar or jimmy, or it can be sawed or cut by bolt cutters. The casing can be crushed or distorted by hammering. Modifications have been incorporated into better padlocks to reduce their vulnerability to these approaches. Heavy, hardened steel cases and shackles are used to defeat cutting and crushing. Rotating inserts and special hardened materials are used to prevent the sawing of shackles. Toe and heel locking is used to prevent prying (Figure 7-22).

High-security padlocks are large and heavy, using hardened metals in the case, and a thick, hardened, and protected shackle. Positive locking methods are always used. As little of the shackle is exposed to attack as possible in the locked position. A typical high-security padlock is shown in Figure 7-21. This is the shackleless padlock, which is designed so that a locking bar which is contained entirely inside the case is used in the place of an exposed shackle. This is sometimes called a hasp lock rather than a padlock.

A padlock is, however, no better than the hasp it engages. Hasps offering reasonable security are made of hardened metals. They must be properly mounted on solid materials so that they cannot be pried off. In the locked position, no mounting screw or bolt should be accessible. Padlocks and hasps should always be considered as a unit. There is no point in mounting a high-security padlock on an inferior hasp. The hasp and lock should always be about the same quality. Where they are not, the complete device is only as good as its weakest member.

STRIKES

Strikes are an often overlooked but essential part of a good lock. A dead bolt must engage a solid, correctly installed strike, or its effectiveness is significantly reduced. The ordinary strike for residential use is mounted with two or three short (usually less than 1 inch) wood screws on a soft wood door frame. It can be easily pried off with a screwdriver. High-security strikes are wider and longer and often incorporate a lip that wraps around the door for added protection against jimmying and shimming (Figure 7-23). Three or more offset wood screws at least 3½ inches long are used to mount the strike. These screws must extend through the jamb and into the studs of the door frame. This provides added protection against prying attacks. Additionally, none of the fastening screws should be in line. In-line screws tend to split soft wood when they are screwed in. Strikes designed for installation on wood frames should always use offset screws as fasteners.

Reinforced steel should be used on metal-framed doors, especially aluminum frames. Aluminum is an extremely soft metal and, unless a reinforced strike is used, the jamb can be peeled away from the strike area, exposing the bolt to a number of attacks or allowing it to clear the jamb thereby freeing the door to open. Bolts should be used to mount strikes in metal frames. If the bolt does not penetrate a substantial steel framing member, then a steel plate should be used to back the bolt (very large steel washers may be

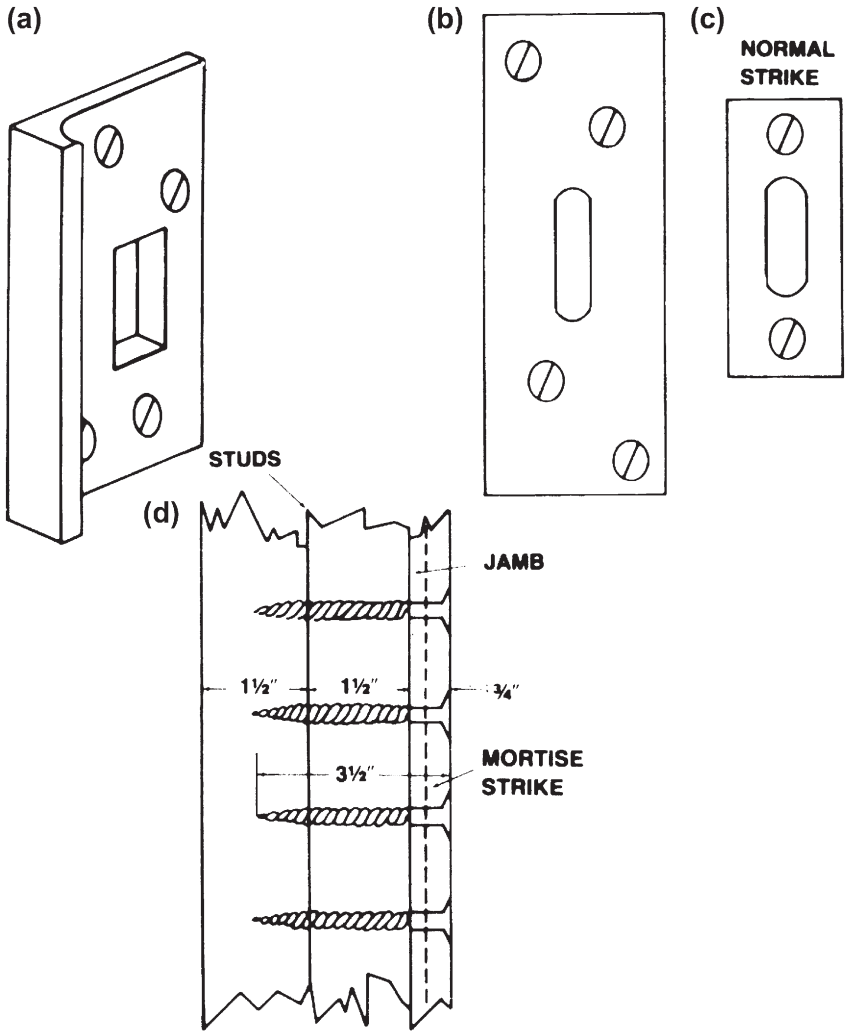


FIGURE 7-23 High-security strikes: (a) security strike with reinforced lip to prevent jimmying and shimming, (b) security strike for wood frames with offset screws, (c) normal strike, and (d) proper installation of a strike on a wood frame.

an acceptable substitute). This prevents the strike from being pried out of aluminum or thin steel frames.

ATTACKS AND COUNTERMEASURES

There are two basic methods of attacking locks: surreptitious techniques and force. There are also a number of ways of circumventing a lock by assaulting the objects to which it is fastened. This chapter will be concerned only with techniques used to defeat locks and the measures that can be used to forestall those techniques.

No lock is completely invulnerable to attack. A lock's effectiveness is determined by how long it will resist the best effort of an intruder. An expert can pick an average pin tumbler cylinder in seconds, and no lock can survive strong force applied for a sufficient length of time. The sole object of using any lock at all is to *delay* an intruder. A good lock makes entry riskier or more

trouble than it is worth, and that is the objective. Fortunately, most potential intruders are not experts, thus most moderately secure locks can survive for a reasonable amount of time against common attack techniques.

The proper use of countermeasures will significantly reduce a locking system's vulnerability to breaching by an unauthorized person. However, not all of the countermeasures suggested in the following sections will be appropriate for every application. There is always the necessity of striking a suitable compromise between the expense and inconvenience of a locking system and the value of the items it is designed to protect. Complex and expensive very high security systems are simply not appropriate for most residential applications. On the other hand, a cheap padlock on a warehouse containing valuable merchandise is an open invitation for someone to break in and steal it. The objective should always be to ensure reasonable protection in the circumstances surrounding a particular application. With locks, overprotection is often more harmful than insufficient protection. If the user is faced with a more complex security system than is really necessary, she or he simply will not use it. A great many unlawful entries are still made through *unlocked* doors and windows. The temptation to avoid the inconvenience of constantly locking and unlocking barriers seems to be insurmountable for some people. Contributing to this temptation by insisting on more protection than the user actually needs simply aggravates the problem.

Surreptitious Attacks

Four basic surreptitious approaches are used to breach locking devices: illicit keys, circumvention of the internal barriers of the lock, manipulation of the internal barriers, and shimming. The susceptibility of any locking device to these approaches cannot be eliminated but can be minimized through the use of commonsense countermeasures.

Illicit Keys. The easiest way of gaining entry through any lock is by using the proper key for that lock. Thousands of keys are lost and stolen every year. A potential intruder who can determine which lock a lost or stolen key fits has a simple and quick means of illicit entry. If an intruder cannot get hold of the owner's key, quite often he or she can make a duplicate. The casual habit of leaving house keys on the key ring when a car is left in a commercial parking lot or for servicing provides a potential intruder with a golden opportunity to duplicate the house keys for later use. One can also find out the owner's address very quickly by examining the repair bill or tracing the automobile license number.

The risk of lost, stolen, or duplicated keys cannot be eliminated entirely, but certain steps can be taken to minimize it.

Maintain Reasonable Key Security

- Under some circumstances, it is almost impossible to avoid leaving at least the ignition key with a parked car, or one to be serviced. But all other keys should be removed.
- When keys are being duplicated, the owner should ensure that no extra duplicates are made.
- Many locks, particularly older locks, have their key code stamped on the front of the case or cylinder. This permits anyone to look up the code in a locksmith's manual and find the proper combination for that lock (or for that combination lock). Codebooks are readily available for most makes of lock, so if the code appears anywhere on the lock where it can be read after the lock is installed and locked, it should be removed by grinding or overstamping. If removal is not possible, the lock or its combination should be changed.
- Managers and owners of commercial enterprises should maintain strict control over master keys and control keys for removable-core cylinders. The loss of these keys can compromise the entire system, necessitating an extensive and expensive system-wide recombination. Too often in large institutions just about everyone can justify a need for a master key. This is nothing more than a demand for

convenience that subverts the requirements of good security. The distribution of master keys should be restricted to those who literally cannot function without them.

Since it is impossible to prevent people from losing keys no matter how careful they are, the next precaution is to *ensure that the lost key cannot be linked to the lock it operates*.

- The owner's name, address, telephone number, or car license number should never appear anywhere on a key ring. This has become common practice to ensure the return of lost keys, but if they fall into the wrong hands, the address provides a quick link between the keys and the locks they fit. The proper protection against lost keys is to always have a duplicate set in a secure place.
- For the same reasons, keys stamped with information that identifies the location of the lock should not be carried around. This used to be a common practice on locker keys, safety deposit box keys, and some apartment building keys. It is no longer as common as it once was, but it still exists. If the keys must be carried, all identifying information should be obliterated, or they should be duplicated on a clean, unmarked key blank.

Recombinate or Replace Compromised Locks. If all these precautions fail and the owner reasonably believes that someone has obtained keys to her or his locks, the combinations of these locks should be changed immediately. Where this is not possible, the locks may have to be replaced. When only a few locks are involved, recombinating cylinders is a fairly quick and inexpensive operation well within the competence of any qualified locksmith.

Another common attack method using a key against which there is less direct protection is the *try-out key*. Try-out key sets are a common locksmith's tool and can be purchased through locksmith supply houses, often by mail. These sets replicate the common variations used in the combination of a particular lock series. In operation, they are inserted into the lock one at a time until one is found that will operate the lock.

Try-out keys are commercially available only for automotive locks. There is nothing, however, to prevent a would-be intruder from building a set for other locks. In areas where one contractor has built extensive residential and commercial developments, most of the buildings will often be fitted with the same lock series. If it is an inexpensive series with a limited number of useful combinations, a homemade try-out key set that replicates the common variations of this particular lock series could be very useful to the potential intruder.

The defense against try-out keys is simply to use a lock with a moderate to high number of available combinations. Any lock worth using has at least several thousand useful combinations. No intruder can carry that many try-out keys, so the risk that he or she will have the proper key is minimal.

Circumvention of the Internal Barriers of the Lock

This is a technique used to directly operate the bolt *completely bypassing* the locking mechanism that generally remains in the locked position throughout this operation. A long, thin stiff tool is inserted into the keyway to bypass the internal barriers and reach the bolt assembly. The tool (often a piece of stiff wire) is then used to maneuver the bolt into the retracted, unlocked position. Warded locks are particularly vulnerable to this method (as was indicated earlier), but some tumbler mechanisms with an open passageway from the keyway to the bolt assembly are also susceptible. Some older padlocks and cylindrical mechanisms had an open passageway of this sort. Few of these are manufactured anymore, but some of the older models are still in use. Any lock that has this type of an opening should be replaced with a better device if reasonable security is a requirement.

Manipulation

The term manipulation covers a large number of types of attacks. At least 50 discrete techniques

of manipulating the mechanism of a lock without the proper key have been identified. Fortunately, however, they all fall rather neatly into four general categories: *picking*, *impressioning*, *decoding*, and *rapping*. Regardless of the specific technique used, its purpose is to maneuver the internal barriers of a tumbler mechanism into a position where they will permit the bolt to be retracted. In a disc or pin tumbler mechanism, this means that the cylinder plug must be freed to rotate; in a lever lock, the levers must be aligned with the fence.

The basic countermeasures against all forms of manipulation are the use of close tolerances in the manufacture of the mechanism and increasing the number of pins, discs, or levers. Close tolerances and a large number of tumblers make manipulation a time-consuming process. A number of specific defenses to the various forms of manipulation have also been developed. These will be presented in some detail in the following sections.

Picking. Lock picking is undoubtedly the best known method of manipulation. It requires skill developed by dedicated practice, the proper tools, time, and often a small dose of good luck. No lock is pick proof, but the high-security locks are so difficult to pick that it takes even an expert a long time to open them. One definition of a high-security mechanism, in fact, is one that cannot be picked by an expert in less than half a minute.

The techniques involved in picking the three basic types of tumbler mechanisms are very similar that an example using the pin tumbler cylinder will serve to illustrate the rest.

All picking techniques depend on the slight clearances that must necessarily exist in a mechanism for it to function. The basic technique requires slight tension to be placed on the part of the mechanism that retracts the bolt (which is the cylinder plug in pin tumbler mechanisms) by a special tension tool designed for that purpose (Figure 7-24). The result of this tension is shown in Figure 7-25. The pin chamber in the plug has moved slightly out of alignment with the pin chamber in the cylinder shell, creating two *lips* at points A and B. When the key pin is pushed up by the pick, it tends to catch at the shear line because the lip at point A permits it to go no farther. This pushes the driver above the shear line where the lip at point B prevents it from falling down into the cylinder plug once more. As long as tension is maintained, it will stay above the shear line.

This operation is facilitated by the fact that, as shown in Figure 7-26, the pin chambers in a cylinder plug are seldom in a perfectly straight line. Consequently, the pin closest to the direction of tension will be more tightly bound than the rest of the pins when tension is applied. It can easily be located because it will offer the most resistance to being maneuvered by the pick. Each pin is tested by lifting it with the pick. The pin that is most resistant is picked first. When this pin reaches the shear line, often the cylinder plug will move slightly. The picker receives two important benefits from this very small movement: first it indicates that the pin has indeed been lifted to the shear line, and second, the movement of the cylinder increases the misalignment between the pin chamber in the plug and the one in the shell, making it even less likely that the driver will drop down into the plug (Figure 7-27). Once this pin has been picked, the next pin nearest the direction of tension will be the most tightly bound. It is located and picked next. The cylinder plug will again move a very small amount. This operation continues until all of the pins are picked above the shear line and the cylinder plug is free to rotate.

There are endless variations of this basic picking technique. One of the most common is the use of a *rake pick*. When this pick is used, very slight tension is applied to the plug, and then the rake is run along the tumblers lifting them slightly each time until all of them reach the shear line. Raking increases the chance that one or more key pins will inadvertently be pushed up into the cylinder shell, which will not allow the plug to rotate. It is often necessary to release the tension applied to the plug and start over again several times. Nevertheless, it is a very fast technique, and very popular. With luck, an expert using a rake can pick an average pin tumbler in a few seconds.

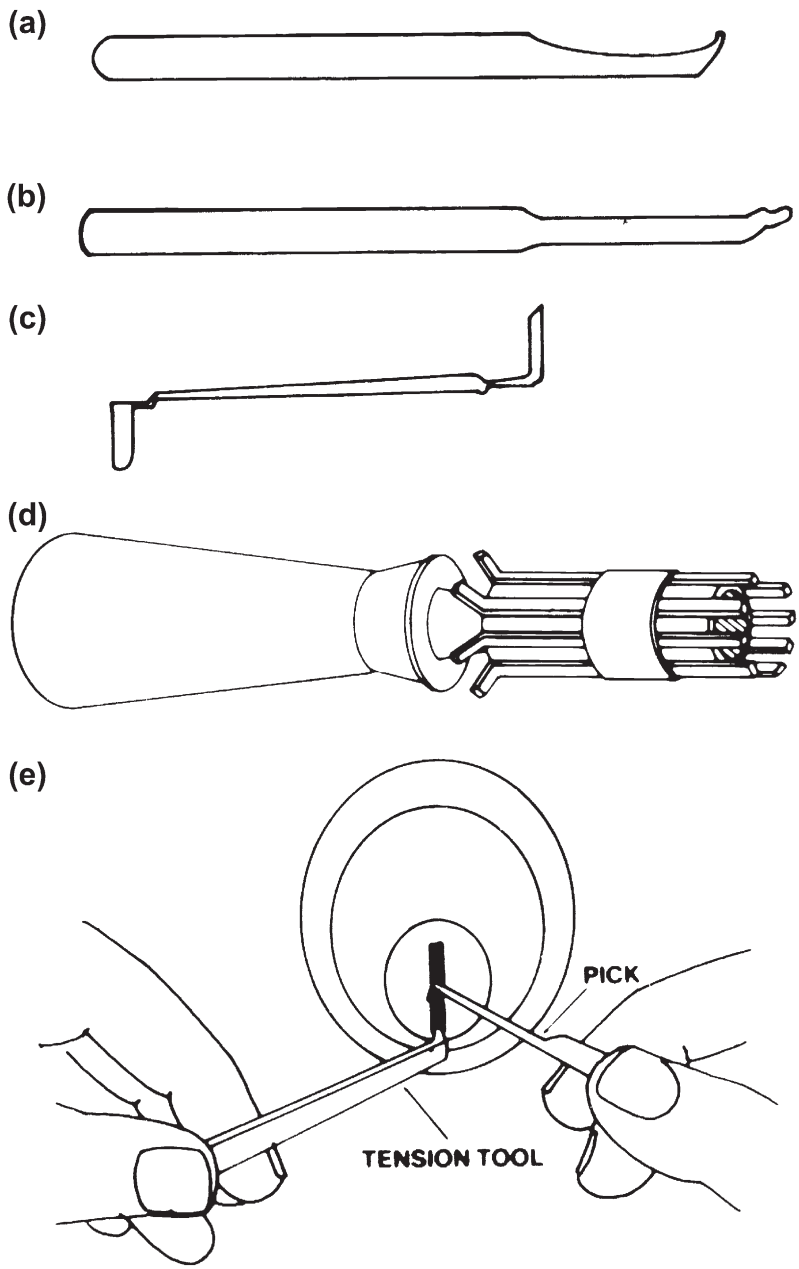


FIGURE 7-24 Lock picks: (a) standard pick, (b) rake pick, (c) tension tool, (d) special pick for tubular mechanisms, and (e) pick and tension tool in use.

Most of the improvements in lock technology made over the last few thousand years have been devoted to increasing the resistance of locks to picking. The major defense is the use of very close tolerances in the mechanism during manufacture. This makes the forced misalignment between the plug and shell necessary for successful picking more difficult to achieve. The addition of more

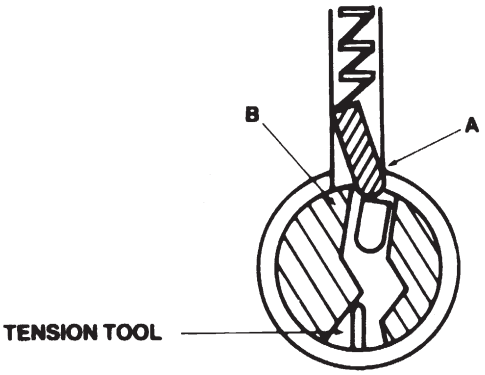


FIGURE 7-25 Illustration of the misalignment caused in a pin tumble cylinder when tension is applied.

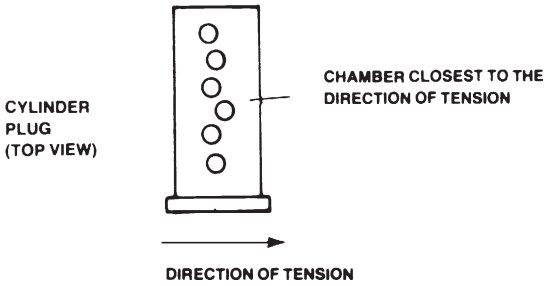


FIGURE 7-26 Pin chamber misalignment. Pin chambers on even the best cylinders are not in a perfectly straight line. The misalignment in this illustration is highly exaggerated for clarity.

tumblers is also some protection against picking, since it takes the operator more time to pick all of the tumblers in the mechanism. The Sargent Keso mechanism and the Duo disc tumbler use this basic approach. The 12 pins in the former and 14 (soon to be 17) discs in the high-security (UL listed) Duo take a reasonably long time to pick successfully. In addition, the unusual configurations of these tumblers make picking even more difficult.

The unusual arrangement of tumblers is also a basic security feature of Ace (tubular) mechanisms. These cannot be picked using ordinary picks, but there are special tools available that facilitate picking this lock. The Ace lock also requires special skills, but these are not too difficult to achieve once basic picking techniques have been mastered.

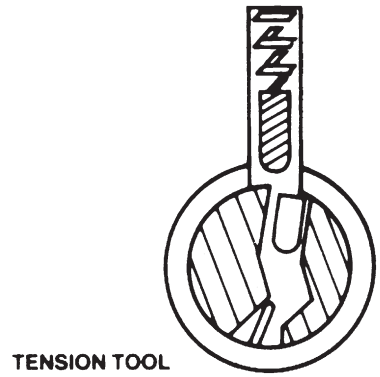


FIGURE 7-27 Increased misalignment occurs as each pin is picked.

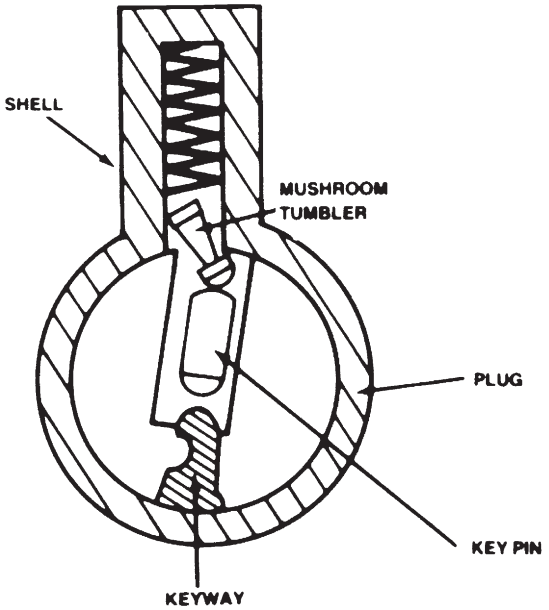


FIGURE 7-28 Mushroom and spool tumblers tend to bind in the pin hole when manipulation is attempted.

Modifications of pin design for increased resistance to picking (and other forms of manipulation) are becoming increasingly important as a basic means of precluding this form of attack. As shown in Figure 7-28, mushroom, spool, and huck pins tend to bind in the pin chamber when tension is applied to the cylinder plug, preventing the key pin from reaching the shear line. The use of these pins does not provide an absolute

defense against picking attempts, but a steady hand and a great deal of skill are required to pick them successfully.

Pins that must be rotated provide what is perhaps the maximum protection currently available against picking. The Medeco and the new Emhart interlocking mechanism both require pins to be lifted to the shear line *and* rotated to a certain position before the lock will operate. It is very, very difficult to consistently rotate these pins into the correct position. The interlocking pins on the Emhart also make it extremely difficult to pick the key pin to the shear line, since, when interlocked, the two pins act as if they were one solid pin. The key pin and driver will not split at the shear line unless the pins are first rotated to the correct position.

Fewer such embellishments are possible with discs and levers. Most high-security lever locks, however, do use levers that have a front edge cut in a sawtooth design (serrated). These serrations tend to catch on the fence as it is pushed back to provide pressure on the levers. This often makes it necessary for the operator to release tension and start over again, which increases the time spent picking the lock. The use of two sets of levers with two corresponding fences also increases a lever mechanism's resistance to picking attempts.

Impressioning. Impressioning is a technique used to make a key that will operate the lock. It cannot ordinarily be used against high-security mechanisms, but against the average lock it can be very successful.

To make a key by impressioning, a correct key blank is inserted into the lock. It is then securely gripped by a wrench or pliers (there are also special tools available for this purpose) and a strong rotational tension is applied to the plug. While this tension is applied, the key is moved up and down in the keyway. Since the tumblers are tightly bound in the lock by the tension applied to the plug, they will leave marks on the blank. The longest key pin will leave the strongest impression. The key is then removed and a slight cut is filed in the blank. The top of the key is smoothed down with a file or abrasive paper, and the key is again inserted to pick up the impression of the next longest pin. As long as the pin leaves an impression, the cut is deepened. When the pin will no longer leave a mark, the cut is at the right depth. When all of the cuts are to the right depth, the key will operate the lock and permit entry.

Certain types of lock mechanisms are more susceptible to impressioning than others. Warded locks are easily defeated by this method since the fixed wards can be made to leave strong impressions, and, as previously stated, the depth of the cut on a warded key is not critical. Lever locks are probably the most immune to this technique, since it is difficult to bind the levers in such a manner that they will leave true impressions on the key blank. The use of serrated levers greatly increases this difficulty.

The average pin and disc tumbler mechanism is vulnerable to this approach, but some of the better high-security mechanisms, because of their unusual keys, are not. The Medeco and Emhart interlocking mechanisms are highly resistant. The correct angles of the slant cuts necessary on these keys cannot be determined by impressioning. The special design of the pins in the BHI Huck-Pin cylinder makes the pins bind almost anywhere in the pin hole except at the shear line. All of the impressions that appear on the key blank are, therefore, likely to be false impressions. So, although this mechanism uses a fairly standard paracentric key, it is still very difficult to defeat by impressioning. Modified spool and mushroom tumblers in any pin tumbler mechanism also tend to increase the difficulty of getting good impression marks.

Decoding. Another method of making a key for a particular lock is through decoding. It was mentioned earlier that most disc tumbler mechanisms can be sight read fairly easily. Sight reading involves the manipulation of the tumblers with a thin wire while noting their relative positions in the keyway. Since each mechanism has only a limited number of possible tumbler increments, the correct alignment of these increments can be estimated with fair accuracy, permitting a key to be filed or cut on the spot to rotate the lock. This is one method of decoding.

A more common method is to insert a decoding tool or a specially marked key blank for a short distance into the keyway of a pin or disc tumbler mechanism. Using the key, rotational tension is applied to the plug, which causes misalignment between the pin chambers in the plug and shell. The key is then slowly inserted into the keyway until it has forced the first tumbler to the shear line (Figure 7-29). The length of this first key pin is determined by the distance the blank (or special tool) enters the keyway. The blank is then moved to the second tumbler, and so on until the length of all of the tumblers is determined and a key can be cut.

Pin tumbler cylinders having wide tolerances, which are the mechanisms that are most susceptible to this particular decoding method. Disc tumblers are less so, although most can easily be sight read. (The Duo, however, is very resistant to sight reading.) Lever locks require special equipment to decode.

The special features offered on some high-security pin tumbler systems dramatically increase their resistance to this technique. Some are almost immune. The Ace can be decoded, but it usually requires special tools. The use of mushroom or spool tumblers in almost any mechanism increases its resistance to decoding. And, of course, the close tolerances of any of the better mechanisms are a basic defense against decoding as well as impressioning and picking.

Rapping. This approach relies on the fact that pins in a tumbler mechanism can move freely in the pin chambers. Tension is applied to the plug, resulting in the usual misalignment between the core and shell pin bores. The lock is then struck with a sharp tap just above the tumblers. This causes the pins to jump in their bores. As each key pin reaches its shear line, it pushes the driver before it into the shell where it tends to bind, unable to drop back down into the plug because of the lip caused by the misalignment. Not all of the drivers will be pushed over the shear line by one rap. Several may be required.

Theoretically, almost any lock may be defeated by rapping, but in practice it is a method that is used primarily on padlocks. Since padlocks are not encased in a door, they respond more freely to rapping. Modified, manipulation-resistant pins make rapping very difficult, but not impossible; it is, nevertheless, not a practical approach to high-security padlocks, which use close tolerances and modified pins.

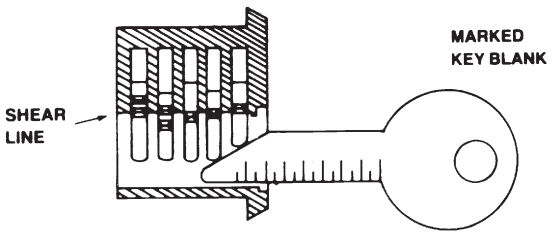


FIGURE 7-29 Decoding using a marked key blank.

Shimming

Any part of a locking mechanism that relies on spring pressure to hold it in place is vulnerable to shimming unless it is protected. Spring-loaded latch bolts can be shimmed by a thin plastic or metal tool unless they are protected by antishim devices. The locking dogs in padlocks are susceptible to a shim inserted into the shackle hole. The shim acts to force the dog back against the spring pressure releasing the shackle. Padlocks that use heel and toe locking are more difficult to shim, but the safest course to use is a nonsprung, positive locking system that cannot be threatened by shimming.

Forceful Attacks. If a potential intruder does not have the skills necessary to decode, impression, or pick a lock, the only course is to find a key or use force against the lock to disable and breach it. Comparatively few intruders have developed manipulative skills, so it is not surprising that the large majority of attacks on locks employ force of one kind or another. Locks can be punched, hammered, wrenched, twisted, burned, pulled, cut, exploded, and pried. Given the right tools and a sufficient amount of time, any lock can be defeated by force. But the nature of forceful attacks entails a number of real disadvantages to an intruder who is trying to gain entry without being discovered in the

process. Large and cumbersome tools that are difficult to carry and conceal are often required. This is especially true if one of the better protected locks is being attacked. Secondly, forceful attacks usually make a considerable amount of noise. Noise, especially unusual noise, tends to prompt people to investigate. Third, it is always immediately evident to even a casual observer that the lock has been attacked. When surreptitious techniques are used, the lock can be opened without damage and relocked, and no one will be able to tell that an unlawful entry has taken place. This often permits the intruder to thoroughly cover tracks even before an investigation is started.

The object of countermeasures against forceful attacks is to increase these hazards. Generally more force will have to be applied to stronger, better protected locks, requiring larger and more sophisticated tools, taking more time, making more noise, and leaving more evidence that the lock has been defeated.

While it is sometimes possible to wrench, pry, or pull an entire lock out of a door, most attacks are directed at either the bolt or the cylinder. If the bolt can be defeated, the door is open. If the cylinder can be defeated, the bolt can be maneuvered into an unlocked position. The common type of attack will be presented in the next section, along with measures that can be taken to strengthen a lock against them. It bears repeating that no lock is absolutely immune to forceful attacks. The object is to make its defeat more difficult, noisier, and more time-consuming, increasing the chances that an intruder will be detected or simply give up before successfully breaching the lock.

Attacks on Bolts

Bolts can be pried, punched, and sawed. The object of these attacks is to disengage the bolt from the strike.

Jimmying and Prying. A jimmy is by definition a short prying tool used by burglars. It is a traditional and well-known burglary tool, but other, more lawful, prying tools will work just as well if not better. These include: pry bars, crowbars, nail pullers, and large screwdrivers.

The easiest prying attack is against latch bolts with antishim devices. A screwdriver or similar tool with a flat blade is inserted between the strike and latch bolt. Pressure is applied until the antishim mechanism inside the lock breaks. The latch is then easily pushed into the retracted position and the door is open. A supplementary long-throw or interlocking dead bolt is the best defense against this attack. Noninterlocking, long-throw dead bolts are theoretically vulnerable to jimmying, but it takes a much larger tool, more time, and the destruction or spreading of part of the door jamb so that the end of the dead bolt can be reached with the prying tool. Even then, a great deal of force is required to push the bolt back into the lock and free the door. These combined disadvantages make direct jimmying attacks against long-throw dead bolts very impractical. They are even more impractical against interlocking dead bolts. If the lock and strike are properly installed, the whole strike would have to be pried loose. This would ordinarily entail the destruction of a considerable portion of the jamb around the strike.

A dead bolt also can be attacked indirectly by prying. An attempt is made to spread the door frame so that the bolt is no longer engaging the strike (Figure 7-30). An average man can apply about 600 inch-pounds of force using a pry bar 30 inches long. This is usually more than enough to spread a door jamb to clear the normal 72-inch bolt, but a 1-inch (or longer) bolt is more difficult to clear. Interlocking bolts are almost impossible to defeat with this method since they, in effect, anchor the door to the door frame. To spread the frame, the entire strike would have to be pried out. A properly installed security strike is very difficult to remove. Interlocking deadbolts were designed to resist just this type of attack. By and large, they are successful. When properly installed they are, as a practical matter, virtually immune.

Automobile bumper jacks (or similar tools) can also be used to spread a door jamb and release the bolt (Figure 7-31). Most American

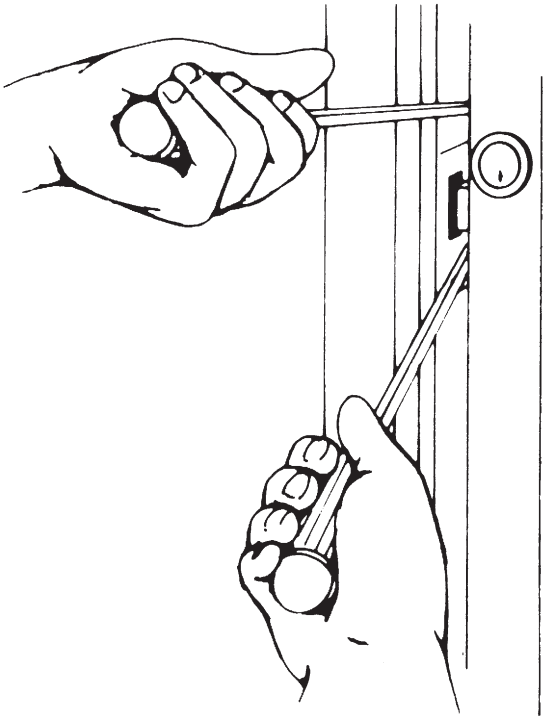


FIGURE 7-30 Jamb spreading by prying with two large screwdrivers.

jacks are rated at 1 ton. It is probably safe to say that most wooden door frames will succumb to that much force. Reinforced metal frames are more resistant. Long-throw and interlocking dead bolts provide some protection. They may even provide enough protection in most circumstances, since a jamb can only be spread so far by the jack before it buckles outward releasing the jack. The best defense against jamb spreading, however, is a properly constructed and reinforced door frame.

Fortunately, this type of attack is fairly rare. An automobile jack is an awkward tool, hard to carry and conceal, and it requires some time to set up and operate.

Punching. The California Crime Technological Research Foundation (CCTRF) identified punching as a possible direct attack on a dead bolt (Figure 7-32). The attacker would have to punch through the wall and framing members to reach the bolt. It would be fairly easy to miss the bolt on the first few tries, so several attempts may be necessary. In essence, the punch and hammer are used to force the bolt back into the body of the lock, allowing it to clear the strike. CCTRF determined that an average man can apply a force of 125 inch-pounds with a 1-pound hammer.

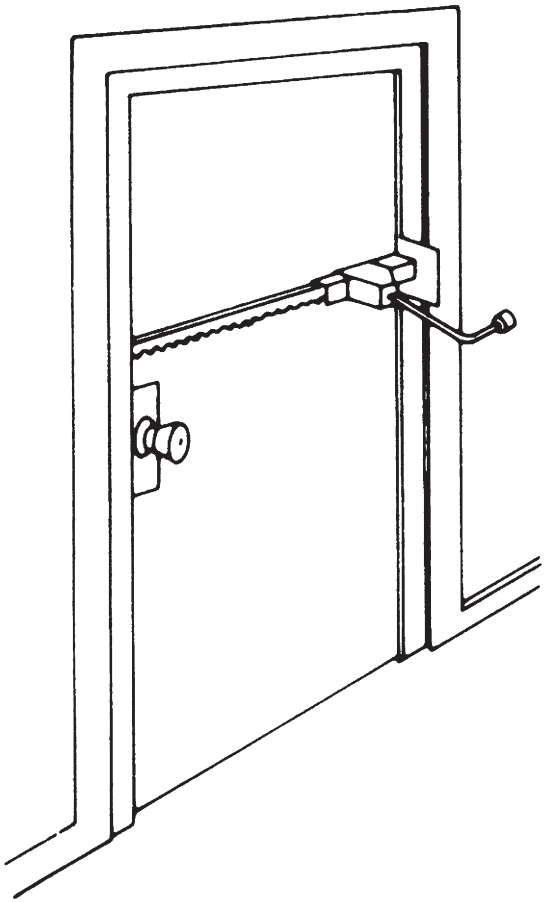


FIGURE 7-31 Use of an automobile bumper jack to spread the door frame. Standard bumper jacks are rated to 2,000 pounds. The force of the jack can be applied between the two jambs of a door to spread them and overcome, by deflection, the length of the latch throw.

Most bolts will probably succumb to a determined punching attack. But it is a noisy approach, and rather hit or miss since it is somewhat difficult to tell if the punch is actually engaging the bolt, and the punch has a tendency to be a serious disadvantage to an intruder, making this an attack of last resort.

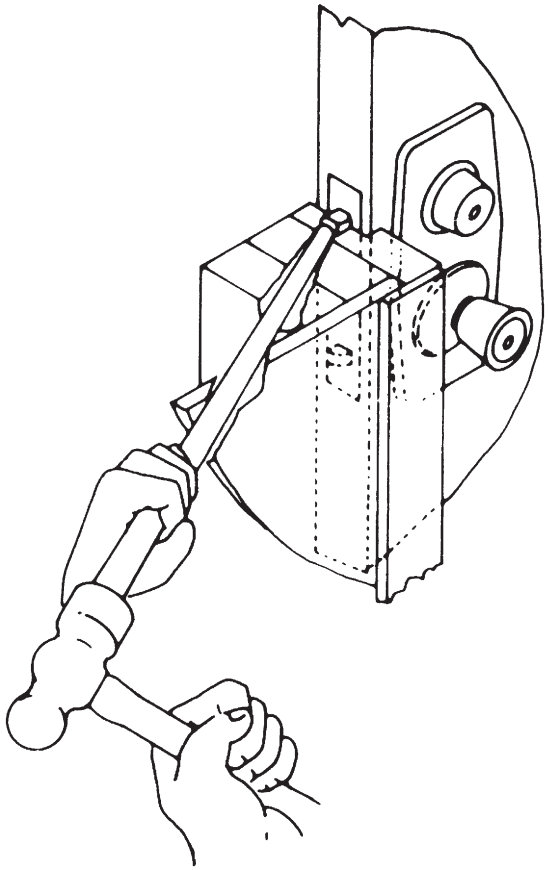


FIGURE 7-32 Forcing the dead bolt with a drift punch and hammer.

Sawing. Bolts can be sawed by inserting a hacksaw or hacksaw blade between the face plate and the strike. (A portion of the jamb will usually be removed or the jamb spread to allow easy access.) Better locks now use hardened bolts or hardened inserts inside the bolt to resist sawing. An even better defense are free-wheeling rollers placed inside the bolt. When the saw reaches these rollers, the sawing action rolls them back and forth but will not cut them. Modified bolts are present in almost all relatively secure locks, and they are virtually immune to sawing attacks.

Peeling. Another way to expose the bolt in metal-framed doors is by peeling. Thin sheet steel and aluminum can be easily peeled. The normal countermeasure against this attack is to use a reinforced strike. Peeling may also be used with prying in an attempt to force the bolt back into the lock.

Attacks on Cylinders

Like bolts, cylinders can be pried and punched. They also can be drilled, pulled, wrenched, or twisted. The usual objective of such attacks is to completely remove the cylinder from the lock. Once it has been removed, a tool can be inserted into the lock to quickly retract the bolt.

Cylinder Pulling. The tool usually used for cylinder pulling is a slam hammer or dent puller—a common automobile body shop tool ordinarily used to remove dents from car bodies. The hardened self-tapping screw at the end of the puller is screwed into the keyway as far as it will go. The hammer is then slammed back against the handle. More often than not, an unprotected cylinder will be yanked entirely out of the lock with one or two slams. CCTRF determined that 200 inch-pounds of force could be applied to a cylinder by a dent puller using a 2½-pound hammer having an 8-inch throw.

Many cylinders are vulnerable to this kind of attack because they are poorly anchored in the lock. Mortise cylinders, for example, are ordinarily threaded into the housing and held in place with a small set screw. The threads are usually soft brass or cast iron. A good yank shears both these threads and the set screw.

Most tubular and rim cylinders are held in place by two (or more) bolts inserted from the rear of the lock. This is a much more secure method of retaining the cylinder and one which resists pulling. Retaining bolts of at least ¼ inch in diameter made of hardened steel are good protection against most pulling attempts.

The threat of pulling can be significantly reduced by the addition of a cylinder guard. Some better lock assemblies are offered with built-in guards. Locks that do not have a built-in guard can be protected with a bolt-on guard. These are bolted over the cylinder using carriage bolts that extend completely through the door (Figure 7-33). They offer the maximum available

resistance to pulling. The cylinder guard, when correctly mounted, cannot be pried off without virtually destroying the entire door.

Cylindrical (lock-in-knob) locksets are extremely vulnerable to pulling. Often the doorknob will be pulled off with the cylinder, exposing the entire internal mechanism to manipulation. There is no method of reinforcing a cylindrical lockset against the threat of pulling. The best measure is to replace it or add a good supplementary deadlock with a cylinder guard.

Lug Pulling. If the cylinder is protected against pulling, an attacker may turn to the cylinder plug. The plug is much harder to pull, and requires a special tool that looks something like a gear puller. A hardened self-tapping screw is engaged in the keyway and pressure is slowly exerted on the plug until the tumblers snap and the plug can be pulled from the cylinder shell. The bolt mechanism can then be operated by a tool inserted through the shell. The ordinary cylinder guard is no protection against this attack. A special guard is available, however, which is designed to prevent the plug from being pulled (see Figure 7-34).

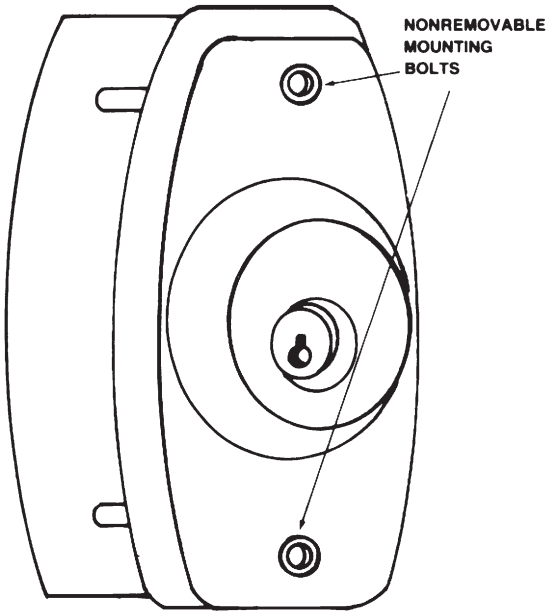


FIGURE 7-33 Bolt-on cylinder guard with back plate. This commercially available plate is of heavy aluminum and is mounted from the inside of the door with hardened steel bolts that enter threaded holes in the guard. It combines good protection with good appearance.

Wrenching, Twisting, and Nipping. Most cylinders project from the surface of the door sufficiently to be gripped by a pipe wrench or pliers. Twisting force is applied to the cylinder by the wrench, which is often sufficient to snap or shear the set-screws or bolts that hold the cylinder in the lock. If the cylinder does not project enough for a wrench to be used, a ground-down screwdriver can be inserted in the keyway and twisting force applied to the screwdriver with a wrench. CCTRF found that an 18-inch-long pipe wrench could apply a maximum torque of 3,300 inch-pounds to a protruding cylinder housing, and a screwdriver turned with a wrench could produce 600 inch-pounds.

The proper protection against this threat once again is a cylinder guard. Some of the built-in guards are free-wheeling, which prevents a twisting force from being successfully applied. Those that are not free-wheeling are still made of hardened steel, which does not allow the wrench to get a good bite, but more important, it prevents the wrench from reaching the actual cylinder. If a screwdriver and wrench are used, the cylinder might be twisted loose, but it cannot be pulled out. Although the lock might be damaged, it will not be defeated.

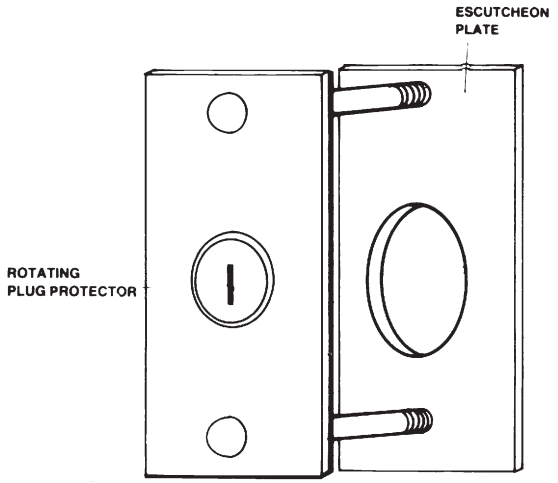


FIGURE 7-34 Cylinder guard with rotating plug protector.

Bolt nippers also can be used to remove protruding cylinders by prying and pulling. Cylinder guards also forestall this type of attack.

Cylindrical locksets are very susceptible to wrenching, twisting, and nipping attacks. Some of the better cylindrical devices have free-wheeling doorknobs that provide some protection against wrenching and twisting. Some incorporate breakaway knobs, which do not expose the internal mechanism of the lock when the knob is twisted off. Nevertheless, combinations of twisting, pulling, and hammering attacks usually quickly defeat these devices. The best remedy is to replace cylindrical mechanisms or supplement them with guarded deadlocks.

Drilling. Cylinder plugs can be drilled out using a fairly large drill bit, but the most common drilling attack is centered on the shear line between the plug and shell (Figure 7-35). A smaller bit is used to drill through the pins, creating a new shear line and releasing the plug, which can then be rotated using a screwdriver or key blank in the keyway. Most of the better locks incorporate hardened inserts to frustrate drilling. Any lock receiving UL approval incorporates these features. Hardened materials do not prevent drilling, but drilling through tempered steel is a long and slow process, which greatly increases the chances of detection.

BHI's Huck-Pin cylinder has an added protection against drilling. When most cylinders are drilled at the shear line, the drivers will fall out of the shell into the plug, releasing the plug to rotate. BHI's drivers are flanged, which prevents them from falling out, so they still effectively lock the mechanism after it is drilled. This does not prevent the entire cylinder from being drilled out, but this is an even longer and slower process than drilling along the shear line.

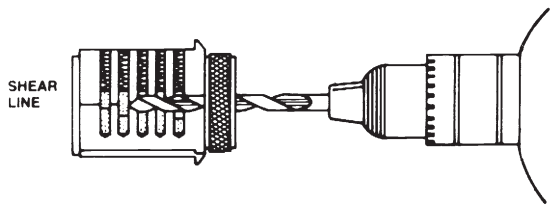


FIGURE 7-35 Drilling.

Punching. Rim-mounted deadlocks are particularly vulnerable to punching. These are ordinarily mounted on the back of a door with wood screws. But, since most of the currently available doors are made with particle board cores under a thin veneer overlay, screws are seldom able to take much pressure. Several good blows with a hammer and punch on the face of the cylinder will often drive it through the door, pulling the screws out, so the entire lock body is dislodged.

Correctly mounting the lock using bolts that extend through the door and engage an escutcheon plate (or even large washers) on the front side generally frustrates punching attacks.

Cylindrical locksets are vulnerable to combination punching and hammering attacks. The knob is first broken off, then the spindle is punched through the lock, exposing the latch bolt assembly to manipulation.

Hammering. Hammering, as well as pulling, wrenching, and twisting, is a quick and very effective way to disable cylindrical locksets. It is not as effective against cylinders, particularly those that are protected by cylinder guards. Ordinarily the knob on a cylindrical mechanism can be quickly broken off by one or two strong blows. There is no direct defense against this type of attack. Again, the only viable solution is a supplementary guarded deadlock, or replacement of the cylindrical lockset with a more secure lock.

LOCKS AND THE SYSTEMS APPROACH TO SECURITY

Locks are an essential part of most security systems. They are, however, only one part. The effectiveness of a lock cannot be considered apart from the effectiveness of the entire system. A lock is no better than the door it is on, or the frame in which the door is mounted. The strongest lock available on a substandard door does not prevent the door from being defeated, even though the lock cannot be.

The degree of protection required from any security system reflects the value of the items to be protected. Most residences require only a modest degree of security—sufficient to thwart the

casual or opportunistic intruder. Jewelry stores, banks, and other establishments, which must keep valuable items on the premises, attract a more determined attacker. The degree of protection for these places must, therefore, necessarily be greater. But whatever the degree of protection required, the actual protection offered by any system is no greater than the vulnerability of its weakest member. A good lock on a poor door provides no more protection than the strength of the door. A good lock on a solid door in a substandard wall is as vulnerable as the wall is weak.

The locks employed in any protection system must complement the system. If a moderate degree of security is required (as in a residential application), a good cylinder properly installed in a secure lock body must be correctly mounted on a good, solid door. The door must be correctly hung, using good hardware, on a properly constructed door frame. The frame must be strongly braced, and secured to the wall. The wall must be at least as strong as the door system installed in it. If the lock, the door, the frame, or the wall is significantly weaker than the rest of the system, it is the point most likely to be successfully attacked.

A good lock is essential to a good security system. It is often the point at which an intruder will focus an attack. But good locks are not synonymous with good security. Always examine the system as a whole.

APPENDIX 7.A. KEY CONTROL*

Eugene D. Finneran

Before an effective key control system can be established, every key to every lock that is being used in the protection of the facility and property must be accounted for. Chances are good that it will not even be possible to account for the most critical keys or to be certain that they have not been copied or compromised. If this is the case, there is but one alternative—rekey the entire facility.

Once an effective locking system has been installed, positive control of all keys must be gained and maintained. This can be accomplished only if an effective key record is kept. When not issued or used, keys must be adequately secured. A good, effective key control system is simple to initiate, particularly if it is established in conjunction with the installation of new locking devices. One of the methods used to gain and maintain effective key control is outlined as follows:

1. **Key cabinet.** A well-constructed cabinet will have to be procured. The cabinet will have to be of sufficient size to hold the original key to every lock in the system. It should also be capable of holding any additional keys that are in use in the facility but are not a part of the security locking system. The cabinet should be installed in such a manner so as to be difficult, if not impossible, to remove from the property. It should be secured at all times when the person designated to control the keys is not actually issuing or replacing a key. The key to the key cabinet must receive special handling, and when not in use it should be maintained in a locked compartment inside a combination-type safe.
2. **Key record**. Some administrative means must be set up to record key code numbers and indicate to whom keys to specific locks have been issued. This record may take the form of a ledger book or a card file.
3. **Key blanks.** Blanks used to cut keys for issue to authorized personnel must be distinctively marked for identification to ensure that no employees have cut their own keys. Blanks will be kept within a combination-type safe and issued only to the person authorized to cut keys and then only in the amount that has been authorized by the person responsible for key control. Such authorization should always be in writing, and records

*Originally from Finneran, ED. Security supervision: A handbook for supervisors and managers. Stoneham, MA: Butterworths, 1981.

should be maintained on each issue, which will be matched with the returned key. Keys damaged in the cutting process must be returned for accountability.

4. **Inventories.** Periodic inventories will have to be made of all key blanks, original keys, and all duplicate keys in the hands of the employees to whom they have been issued. This cannot be permitted to take the form of a phone call to an employee, supervisor, or executive asking if they still have their key. It must be a personal inspection of each key made by the person who has been assigned responsibility for key control.
5. **Audits.** In addition to the periodic inventory, an unannounced audit should be made of all key control records and procedures by a member of management. During the course of these audits a joint inventory of all keys should be conducted.
6. **Daily report.** A daily report should be made to the person responsible for key control from the personnel department, indicating all persons who have left or will be leaving the employ of the company in the near future. A check should be made, upon receipt of this report, to determine whether the person named has been issued a key to any lock in the system. In the event a key has been issued, steps should be initiated to ensure that the key is recovered.

Security force personnel will normally be issued master keys, when such a system is in effect, or they will be issued a ring of keys permitting them to enter any part of the guarded facility. Keys issued to the security force should never be permitted to leave the facility. They should be passed from shift to shift and must be receipted for each time they change hands. The supervisor must ensure that all security personnel understand the importance of not permitting keys to be compromised.

A lost master key compromises the entire system and results in a breakdown of the security screen. Such compromise will necessitate the rekeying of the entire complex, sometimes at a cost of thousands of dollars.

If rekeying becomes necessary, it can most economically be accomplished by installing new locking devices in the most critical points of the locking system and moving the locks removed from these points to less sensitive areas. Of course, it will be necessary to eventually replace all of the locks in the system, but by using the procedure just described the cost can be spread over several budgeting periods.

NEW STANDARD SET FOR EXIT DEVICES, LOCKS, AND ALARMS [1]

The Builders' Hardware Manufacturer's Association (BHMA) has announced a new American National Standard for exit locks and exit alarms for the safety and security of building occupants.

Developed by BHMA, the new standard was recently approved by the American National Standards Institute (ANSI).

In effect, the new standard recognizes the increased importance of locks, alarms, and other devices that control egress from a building. The standard establishes general requirements as well as operational tests and finish tests for these products. In addition, it gives descriptions and type numbers of exit locks and exit alarms.

Revisions include increased performance requirements with respect to the recommended tests and a slam test not part of the earlier standards has been added. Testing of products in accordance with this standard allows for certification to the ANSI/BHMA standard to be established by third-party testing laboratories.

For more information, or to purchase copies of the ANSI/BHMA A156.29 Standard, please visit http://www.buildershardware.com.

REFERENCE

[1] Security Beat [weekly newsletter by publisher of Access Control and Security Systems] 2, no. 7, February 19, 2002.

APPENDIX 7.B. KEY CONTROL AND LOCK SECURITY CHECKLIST*

John E. Hunter

1. Has a key control officer been appointed?
2. Are locks and keys to all buildings and entrances supervised and controlled by the key control officer?
3. Does the key control officer have overall authority and responsibility for issuance and replacement of locks and keys?
4. What is the basis for the issuance of keys, especially master keys?
5. Are keys issued only to authorized personnel? Who determines who is authorized? Is the authorization in writing?
6. Are keys issued to other than installation personnel? If so, on what basis? Is it out of necessity or merely for convenience?
7. Are keys not in use secured in a locked, fireproof cabinet? Are these keys tagged and accounted for?
8. Is the cabinet for duplicate keys regarded as an area of high security?
9. Is the key or combination to this cabinet maintained under appropriate security or secrecy? If the combination is recorded, is it secured?
10. Are the key locker and record files in order and current?
11. Are issued keys cross-referenced?
12. Are current records maintained indicating:
    a. Buildings and/or entrances for which keys are issued?
    b. Number and identification of keys issued?
    c. Location and number of duplicate keys?
    d. Issue and turn in of keys?
    e. Location of locks and keys held in reserve?
13. Is an audit ever made, asking holders to actually produce keys, to ensure that they have not been loaned or lost?
14. Who is responsible for ascertaining the possession of key?
15. Is a current key control directive in effect?
16. Are inventories and inspections conducted by the key control officer to ensure compliance with directives? How often?
17. Are keys turned in during vacation periods?
18. Are keys turned in when employees resign, are transferred, or are fired?
19. Is the removal of keys from the premises prohibited when they are not needed elsewhere?
20. Are locks and combinations changed immediately upon loss or theft of keys or transfer or resignation of employees?
21. Are locks changed or rotated within the installation at least annually regardless of transfers or known violations of key security?
22. Are current records kept of combinations to safes and the dates when these combinations are changed? Are these records adequately protected?
23. Has a system been set up to provide submasters to supervisors and officials on a need basis with facilities divided into different zones or areas?
24. If master keys are used, are they devoid of markings identifying them as master keys?
25. Are master keys controlled more closely than change keys?
26. Must all requests for reproduction or duplication of keys be approved by the key control officer?
27. Are key holders ever allowed to duplicate keys? If so, under what circumstances?
28. Where the manufacturer's serial number on combination locks and padlocks might be visible to unauthorized persons, has this number been recorded and then obliterated?
29. Are locks on inactive gates and storage facilities under seal? Are seals checked regularly by supervisory or key control personnel?
30. Are measures in effect to prevent the unauthorized removal of locks on open cabinets, gates, or buildings?
31. Are losses or thefts of keys and padlocks promptly reported by personnel and promptly investigated by key control personnel?
32. If the building was recently constructed, did the contractor retain keys during the period

*Prepared by John E. Hunter, U.S. National Park Service.

when construction was being completed? Were locks changed since that time? Did the contractor relinquish all keys after the building was completed?

33. If removable-core locks are in use, are unused cores and core change keys given maximum security against theft, loss, or inspection?
34. Are combination lock, key, and key control records safeguarded separately (i.e., in a separate safe or file) from keys, locks, cores, and other such hardware?
35. Are all locks of a type that offers adequate protection for the purpose for which they are used?

APPENDIX 7.C. TERMS AND DEFINITIONS FOR DOOR AND WINDOW SECURITY*

access control A method of providing security by restricting the movement of persons into or within a protected area.

accessible window (1) Residential—any window located within 3.7 m (12 feet) of grade or a building projection. (2) Commercial—any window located within 4.6 m (18 feet) of grade or within 3 m (10 feet) of any fire escape or other structure accessible from public or semi-public areas.

accordion gate See *sliding metal gate*.

ace lock A type of pin tumbler lock in which the pins are installed in a circle around the axis of the cylinder and move perpendicularly to the face of the cylinder. The shear line of the driver and bottom tumblers is a plane parallel to the face of the cylinder. This type of lock is operated with a push key.

active door (or **leaf**) The leaf of a double door that must be opened first. It is used in normal pedestrian traffic. This leaf is usually the one in which a lock is installed.

anchor A device used to secure a building's part or component to adjoining construction or to a supporting member. See also *floor anchor*, *jamb anchor*, and *stud anchor*.

antifriction latch A latch bolt that incorporates any device that reduces the closing friction between the latch and the strike.

applied trim A separately applied molding used as the finishing face trim of a frame.

apron The flat member of a window trim placed against the wall immediately beneath the windowsill.

architectural hardware See *finish builders' hardware*.

areaway An open subsurface space adjacent to a building that is used to admit light or to provide a means of access to the building.

armored front A plate or plates secured to the lock front of a mortised lock by machine screws in order to provide protection against tampering with the cylinder set screws. Also called *armored face plate*.

astragal A member fixed to, or a projection of, an edge of a door or window to cover the joint between the meeting of stiles; usually fixed to one of a pair of swinging doors to provide a seal against the passage of weather, light, noise, or smoke.

auxiliary lock A lock installed on a door or window to supplement a previously installed primary lock. Also called a *secondary lock*. It can be a mortised, bored, or rim lock.

back plate A metal plate on the inside of a door that is used to clamp a pin or disc tumbler rim lock cylinder to the door by means of retaining screws. The tail piece of the cylinder extends through a hole in the back plate.

backset, flush bolt The distance from the vertical centerline of the lock edge of a door to the centerline of the bolt.

backset, hinge On a door, the distance from the stop face to the edge of the hinge cutout. On a frame, the distance from the stop to the edge of the hinge cutout.

backset, lock The horizontal distance from the vertical centerline of the face plate to the center of the lock cylinder keyway or knob spindle.

backset, strike The distance from the door stop to the edge of the strike cutout.

baffle See *guard plate*.

balanced door A door equipped with double-pivoted hardware designed to cause a semi-counterbalanced swing action when it is opened.

*Reprinted courtesy of United States Department of Commerce, National Bureau of Standards.

barrel key A key with a bit projecting from a round, hollow key shank that fits on a post in the lock.

barricade bolt A massive metal bar that engages large strikes on both sides of a door. Barricade bolts are available with locking devices, and are completely removed from the door when not in use.

bead See *glazing bead*.

bevel (of a door) The angle of the lock edge of the door in relation to its face. The standard bevel is 0.32 cm in 5.1 cm (⅛″ in 2″).

bevel (of a latch bolt) A term used to indicate the direction in which a latch bolt is inclined: regular bevel for doors opening in, reverse bevel for doors opening out.

bevel (of lock front) The angle of a lock front when not at a right angle to the lock case, allowing the front to be applied flush with the edge of a beveled door.

bicentric pin tumbler cylinder A cylinder having two cores and two sets of pins, each having different combinations. This cylinder requires two separate keys, used simultaneously, to operate it. The cam or tail piece is gear operated.

bit A blade projecting from a key shank that engages with and actuates the bolt or level tumblers of a lock.

bit key A key with a bit projecting from a round shank. Similar to the barrel key but with a solid rather than hollow shank.

biting See *cut*.

blank An uncut key or an unfinished key as it comes from the manufacturer, before any cuts have been made on it.

blind stop A rectangular molding, located between the outside trim and outside sashes, used in the assembly of a window frame. Serves as a stop for storm, screen, or combination windows and to resist air infiltration.

bolt That part of a lock which, when actuated, is projected (or "thrown") from the lock into a retaining member, such as a strike plate, to prevent a door or window from moving or opening. See also *dead bolt*, *flush bolt*, and *latch*.

bolt attack A category of burglary attack in which force, with or without the aid of tools, is directed against the bolt in an attempt to disengage it from the strike or to break it.

bolt projection (bolt throw) The distance from the edge of the door, at the bolt centerline, to the furthest point on the bolt in the projected position.

bored lock (or **latch**) A lock or latch whose parts are intended for installation in holes bored in a door. See also *key-in-knob lock*.

bottom pin One of a number of pin tumblers that determines the combination of a pin tumbler cylinder and is directly contacted by the key. These are varied in length and usually tapered at one end, enabling them to fit into the "V" cuts made in a key. When the proper key is inserted, the bottom pins level off at the cylinder core shear line, allowing the core to turn and actuate the lock.

bottom rail The horizontal rail at the bottom of a door or window connecting the vertical edge members (stiles).

box strike A strike plate that has a metal box or housing to fully enclose the projected bolt and/or latch.

breakaway strike See *electric strike*.

buck See *rough buck*.

builders' hardware All hardware used in building construction, but particularly that used on or in connection with doors, windows, cabinets, and other moving members.

bumping A method of opening a pin tumbler lock by means of vibration produced by a wooden or rubber mallet.

burglar-resistant glazing Any glazing that is more difficult to break through than the common window or plate glass, designed to resist burglary attacks of the hit-and-run type.

butt hinge A type of hinge that has matching rectangular leaves and multiple bearing contacts, and is designed to be mounted in mortises in the door edge and in the frame.

buttress lock A lock that secures a door by wedging a bar between the door and the floor. Some incorporate a movable steel rod, which fits into metal receiving slots on the door and in the floor. Also called *police bolt/brace*.

cabinet jamb A door frame in three or more pieces, usually shipped knocked down for field assembly over a rough buck.

cam The part of a lock or cylinder that rotates to actuate the bolt or latch as the key is turned. The cam may also act as the bolt.

cam, lazy A cam that moves less than the rotation of the cylinder core.
cam lock See *crescent sash lock*.
cane bolt A heavy cane-shaped bolt with the top bent at right angles; used on the bottom of doors.
case The housing in which a lock mechanism is mounted and enclosed.
casement hinge A hinge for swinging a casement window.
casement window A type of window that is hinged on the vertical edge.
casing Molding of various widths and thicknesses used to trim door and window openings at the jambs.
center-hung door A door hung on center pivots.
center rail The horizontal rail in a door, usually located at lock height to separate the upper and lower panels of a recessed panel type door.
chain bolt A vertical spring-loaded bolt mounted at the top of door. It is manually actuated by a chain.
chain door interviewer An auxiliary locking device that allows a door to be opened slightly, but restrains it from being fully opened. It consists of chain with one end attached to the door jamb and the other attached to a keyed metal piece that slides in a slotted metal plate attached to the door. Some chain door interviewers incorporate a keyed lock operated from the inside.
change key A key that will operate only one lock or a group of keyed-alike locks, as distinguished from a master key. See also *keyed-alike cylinders* and *master key system*.
changes The number of possible key changes or combination changes to a lock cylinder.
checkrails The meeting rails of double-hung windows. They are usually beveled and thick enough to fill the space between the top and bottom sash due to the parting stop in the window frame.
clearance A space intentionally provided between components to facilitate operation or installation, to ensure proper separation, to accommodate dimensional variations, or for other reasons. See also *door clearance*.
clevis A metal link used to attach a chain to a padlock.
code An arrangement of numbers or letters used to specify a combination for the biting of a key or the pins of a cylinder core.
combination (1) The sequence and depth of cuts on a key. (2) The sequence of numbers to which a combination lock is set.
combination doors or windows Storm doors or windows permanently installed over the primary doors or windows. They provide insulation and summer ventilation and often have self-storing or removable glass and screen inserts.
common entry door (of a multiple dwelling) Any door in a multiple dwelling that provides access between the semi-public, interior areas of the building, and the out-of-doors areas surrounding the building.
communicating frame A double-rabbeted frame with both rabbets prepared for single-swing doors that open in opposite directions. Doors may be of the same or opposite hand.
component A subassembly that is combined with other components to make an entire system. Door assembly components include the door, lock hinges, jamb/strike, and jamb/wall.
composite door A door constructed of a solid core material with facing and edges of different materials.
connecting bar A flat metal bar attached to the core of a cylinder lock to operate the bolt mechanism.
construction master keying A keying system used to allow the use of a single key for all locks during the construction of large housing projects. In one such system, the cylinder cores of all locks contain an insert that permits the use of a special master key. When the dwelling unit is completed, the insert is removed and the lock then accepts its own change key and no longer accepts the construction master key.
continuous hinge A hinge designed to be the same length as the edge of the moving part to which it is applied. Also called a *piano hinge*.
coordinator A mechanism that controls the order of closing of a pair of swing doors and used with overlapping astragals and certain panic hardware that require that one door close ahead of the other.
core See *cylinder core*.
crash bar The cross bar or level of a panic exit device that serves as push bar to actuate the lock. See also *panic hardware*.
cremone bolt A surface-mounted device that locks a door or sash into the frame at both the top and bottom when a knob or lever is turned.

crescent sash lock A simple cam-shaped latch that does not require a key for its operation; usually used to secure double-hung windows. Also called a *cam lock*.

cut An indentation made in a key to make it fit a pin tumbler of a lock. Any notch made in a key is known as a cut, whether it is square, round, or V-shaped. Also called *biting*.

cylinder The cylindrical subassembly of a lock, including the cylinder housing, the cylinder core, the tumbler mechanism, and the keyway.

cylinder collar See *cylinder guard ring*.

cylinder core (or plug) The central part of a cylinder, containing the keyway, which is rotated to operate the lock bolt.

cylinder guard ring A hardened metal ring, surrounding the exposed portion of a lock cylinder, which protects the cylinder from being wrenched, turned, pried, cut, or pulled with attack tools.

cylinder housing The external case of a lock cylinder. Also called the *cylinder shell*.

cylinder lock A lock in which the locking mechanism is controlled by a cylinder. A double cylinder lock has a cylinder on both the interior and exterior of the door.

cylinder, mortise type A lock cylinder that has a threaded housing which screws directly into the lock case, with a cam or other mechanism engaging the locking mechanism.

cylinder, removable core A cylinder whose core may be removed by the use of a special key.

cylinder, rim type A lock cylinder that is held in place by tension against its rim, applied by screws from the interior face of the door.

cylinder ring See *cylinder guard ring*.

cylinder screw A set screw that holds a mortise cylinder in place and prevents it from being turned after installation.

cylindrical lock (or latch) See *bored lock*.

dead bolt A lock bolt that does not have an automatic spring action and a beveled end as opposed to a latch bolt, which does. The bolt must be actuated to a projected position by a key or thumb turn and when projected is locked against return by end pressure.

deadlatch A spring-actuated latch bolt with a beveled end and incorporating a feature that automatically locks the projected latch bolt against return by end pressure.

deadlock A lock equipped with a dead bolt.

deadlocking latch bolt See *deadlatch*.

disc tumbler A spring-loaded, flat plate that slides in a slot that runs through the diameter of the cylinder. Inserting the proper key lines up the disc tumblers with the lock's shear line and enables the core to be turned.

dogging device A mechanism that fastens the cross bar of a panic exit device in the fully depressed position, and retains the latch bolt or bolts in the retracted position to permit free operation of the door from either side.

dogging key A key-type wrench used to lock down, in the open position, the cross bar of a panic exit device.

door assembly A unit composed of parts or components that make up a closure for a passageway through a wall. It consists of the door, hinges, locking device or devices, operational contacts (such as handles, knobs, push plates), miscellaneous hardware and closure, the frame including the head and jambs, the anchorage devices to the surrounding wall, and the surrounding wall.

door bolt A rod or bar manually operated without a key attached to a door to provide a means of securing it.

door check/closer A device used to control the closing of a door by means of a spring and hydraulic or air pressure or by electrical means.

door clearance The space between a door and its frame or the finished floor or threshold, or between the two doors of a double door. See also *clearance*.

door frame An assembly of members surrounding and supporting a door or doors, and perhaps also one or more transom lights and/or sidelights. See also *integral frame*.

door jambs The two vertical components of a door frame called the hinge jamb and the lock jamb.

door light See *light*.

door opening The size of a doorway, measured from jamb to jamb and from floor line or sill to head of frame. The opening size is usually the nominal door size, and is equal to the actual door size plus clearances and threshold height.

door stop The projections along the top and sides of a door frame against which a one-way swinging door closes. See also *rabbeted jamb*.

double-acting door A swinging door equipped with hardware that permits it to open in either direction.

double-bited key A key having cuts on two sides.
double cylinder lock See *cylinder lock*.
double door A pair of doors mounted together in a single opening. See also *active door* and *inactive door*.
double egress frame A door frame prepared to receive two single-acting doors swinging in opposite directions; both doors are the same hand.
double glazing Two thicknesses of glass, separated by an air space and framed in an opening, designed to reduce heat transfer or sound transmission. In factory-made double glazing units, referred to as insulating glass, the air space between the glass sheets is desiccated and sealed airtight.
double-hung window A type of window, composed of upper and lower sashes that slide vertically.
double-throw bolt A bolt that can be projected beyond its first position, into a second, or fully extended one.
double-throw lock A lock incorporating a double-throw bolt.
driver pin One of the pin tumblers in a pin tumbler cylinder lock, usually flat on both ends, which are in line with and push against the flat ends of the bottom pins. They are projected by individual coil springs into the cylinder core until they are forced from the core by the bottom pins when the proper key is inserted into the keyway.
drop ring A ring handle attached to the spindle that operates a lock or latch. The ring is pivoted to remain in a dropped position when not in use.
dry glazing A method of securing glass in a frame by use of a performed resilient gasket.
drywall frame A knocked down (KD) door frame for installation in a wall constructed with studs and gypsum board or other drywall facing material after the wall is erected.
dummy cylinder A mock cylinder without an operating mechanism, used for appearance only.
dummy trim Trim only, without lock; usually used on the inactive door in a double door.
Dutch door A door consisting of two separate leaves, one above the other, which may be operated either independently or together. The lower leaf usually has a service shelf.
Dutch door bolt A device for locking together the upper and lower leaves of a Dutch door.
dwelling unit entry door Any door giving access to a private dwelling unit.
electric strike An electrically operated device that replaces a conventional strike plate and allows a door to be opened by using electric switches at remote locations.
escutcheon plate A surface-mounted cover plate, protective or ornamental, containing openings for any or all of the controlling members of a lock such as the knob, handle, cylinder, or keyhole.
exit device See *panic hardware*.
expanded metal An open mesh formed by slitting and drawing a metal sheet. It is made in various patterns and metal thicknesses with a flat or an irregular surface.
exterior private area The ground area outside a single family house, or a ground floor apartment in the case of a multiple dwelling, that is fenced off by a real barrier and is available for the use of one family and is accessible only from the interior of that family's unit.
exterior public area The ground area outside a multiple dwelling, which is not defined as being associated with the building or building entry in any real or symbolic fashion.
exterior semi-private area The ground area outside a multiple dwelling, which is fenced off by a real barrier, and is accessible only from the private or semi-private zones within the building.
exterior semi-public area The ground area outside a single family house or multiple dwelling, which is accessible from public zones, but is defined as belonging to the house or building by symbolic barriers only.
Face (of a lock) See *face plate*.
face glazing A method of glazing in which the glass is set in an L-shaped or rabbeted frame. The glazing compound is finished off in the form of a triangular bead, and no lose stops are employed.
face plate The part of a mortise lock through which the bolt protrudes and by which the lock is fastened to the door.
fast pin hinge A hinge in which the pin is fastened permanently in place.
fatigue Structural failure of a material caused by repeated or fluctuating application of stresses,

none of which is individually sufficient to cause failure.

fence A metal pin that extends from the bolt of a lever lock and prevents retraction of the bolt unless it is aligned with the gates of the lever tumblers.

fidelity loss A property loss resulting from a theft in which the thief leaves no evidence of entry.

filler plate A metal plate used to fill unwanted mortise cutouts in a door or frame.

finish builders' hardware Hardware that has a finished appearance as well as a functional purpose and may be considered as part of the decorative treatment of a room or building. Also called *finish hardware* and *builders' finish hardware*.

fire stair Any enclosed stairway that is part of a fire-resistant exitway.

fire stair door A door forming part of the fire-resistant fire stair enclosure and providing access from common corridors to fire stair landings within an exitway.

floor anchor A metal device attached to the wall side of a jamb at its base to secure the frame to the floor.

floor clearance The width of the space between the bottom of a door and the rough or finished floor or threshold.

flush bolt A door bolt designed that, when installed, the operating handle is flush with the face or edge of the door. Usually installed at the top and bottom of the inactive door of a double door.

flush door A smooth-surface door having faces that are plain and conceal its rails and stiles or other structure.

foot bolt A type of bolt applied at the bottom of a door and arranged for foot operation. Generally the bolt head is held up by a spring when the door is unbolted.

forced entry An unauthorized entry accomplished by the use of force upon the physical components of the premises.

frame The component that forms the opening of and provides support for a door, windows, skylight, or hatchway. See also *door frame*.

frame gasket Resilient material in strip form attached to frame stops to provide tight closure of a door or window.

front (of a lock) See *face plate*.

gate A notch in the end of a lever tumbler, which when aligned with the fence of the lock bolt allows the bolt to be withdrawn from the strike.

general circulation stair An interior stairway in a building without elevators that provides access to upper floors.

glass door A door made from thick glass, usually heat tempered, with no structural metal stiles.

glass stop See *glazing bead*.

glazing Any transparent or translucent material used in windows or doors to admit light.

glazing bead A strip of trim or a sealant such as caulking or glazing compound, which is placed around the perimeter of a pane of glass or other glazing to secure it to a frame.

glazing compound A soft, dough-like material used for filling and sealing the spaces between a pane of glass and its surrounding frame and/or stops.

grand master key A key designed to operate all locks under several master keys in a system.

grating, bar type An open grip assembly of metal bars in which the bearing bars, running in one direction, are spaced by rigid attachment to cross bars running perpendicular to them or by bent connecting bars extending between them.

grout Mortar of such consistency that it will just flow into the joints and cavities of masonry work and fill them solid.

grouted frame A frame in which all voids between it and the surrounding wall are completely filled with the cement or plaster used in the wall construction.

guard bar A series of two or more cross bars, generally fastened to a common back plate, to protect the glass or screen in a door.

guard plate A piece of metal attached to a door frame, door edge, or over the lock cylinder for the purpose of reinforcing the locking system against burglary attacks.

hand (of a door) The opening direction of the door. A right-handed (RH) door is hinged on the right and swings inward when viewed from the outside. A left-handed (LH) door is hinged on the left and swings inward when viewed from the outside. If either of these doors swings outward, it is referred to as a right-hand reverse (RHR) door or a left-hand reverse (LHR) door, respectively.

handle Any grip-type door pull. See also *lever handle*.

hasp A fastening device consisting of a hinged plate with a slot in it that fits over a fixed D-shaped ring, or eye.

hatchway An opening in a ceiling, roof, or floor of a building, which is large enough to allow human access.
head Top horizontal member of a door or window frame.
head stiffener A heavy-gauge metal angle or channel section placed inside, and attached to, the head of a wide door frame to maintain its alignment; not a load-carrying member.
heel of a padlock That end of the shackle on a padlock that is not removable from the case.
hinge A device generally consisting of two metal plates having loops formed along one edge of each to engage and rotate about a common pivot rod or "pin" and used to suspend a swinging door or window in its frame.
hinge backset The distance from the edge of a hinge to the stop at the side of a door or window.
hinge edge or **hinge stile** The vertical edge or stile of a door or window to which hinges or pivots are attached.
hinge reinforcement A metal plate attached to a door or frame to receive a hinge.
hold-back feature A mechanism on a latch that serves to hold the latch bolt in the retracted position.
hollow core door A door constructed so that the space (core) between the two facing sheets is not completely filled. Various spacing and reinforcing materials are used to separate the facing sheets; some interior hollow-core doors have nothing except perimeter stiles and rails separating the facing sheets.
hollow metal Hollow items such as doors, frames, partitions, and enclosures that are usually fabricated from cold-formed metal sheets, usually carbon steel.
horizontal sliding window A type of window composed of two sections, one or both of which slide horizontally past the other.
impression system A technique to produce keys for certain types of locks without taking the lock apart.
inactive door (or leaf) The leaf of a double door that is bolted when closed; the strike plate is attached to this leaf to receive the latch and bolt of the active leaf.
integral frame A metal door frame in which the jambs and head have stops, trim, and backbends all formed from one piece of material.
integral lock (or latch) See *preassembled lock*.
interior common-circulation area An area within a multiple dwelling that is outside the private zones of individual units and is used in common by all residents and the maintenance staff of the building.
interior private area The interior of a single family house; the interior of an apartment in a multiple dwelling; or the interior of a separate unit within a commercial, public, or institutional building.
interior public area An interior common-circulation area or common resident-use room within a multiple dwelling to which access is unrestricted.
interior semi-public area An interior common-circulation area or common resident-use room within a multiple dwelling to which access is possible only with a key or on the approval of a resident via an intercom, buzzer-reply system.
invisible hinge A hinge so constructed that no parts are exposed when the door is closed.
jalousie window See *louvered window*.
jamb The exposed vertical member of either side of a door or window opening. See also *door jambs*.
jamb anchor A metal device inserted in or attached to the wall side of a jamb to secure the frame to the wall. A masonry jamb anchor secures a jamb to a masonry wall.
jamb depth The width of the jamb, measured perpendicular to the door or wall face at the edge of the opening.
jamb extension The section of a jamb that extends below the level of the flush floor for attachment to the rough door.
jamb peeling A technique used in forced entry to deform or remove portions of the jamb to disengage the bolt from the strike. See *jimmying*.
jamb/strike Component of a door assembly that receives and holds the extended lock bolt. The strike and jamb are considered a unit.
jamb/wall That component of a door assembly to which a door is attached and secured by means of the hinges. The wall and jamb are considered a unit.
jimmying A technique used in forced entry to pry the jamb away from the lock edge of the door a sufficient distance to disengage the bolt from the strike.

jimmy-pin A sturdy projecting screw, which is installed in the hinge edge of a door near a hinge, fits into a hole in the door jamb, and prevents removal of the door if the hinge pins are removed.
keeper See *strike*.
key An implement used to actuate a lock or latch or both into the locked or unlocked position.
key changes The different combinations that are available or that can be used in a specific cylinder.
keyed-alike cylinders Cylinders designed to be operated by the same key. (Not to be confused with master-keyed cylinders.)
keyed-different cylinders Cylinders requiring different keys for their operation.
keyhole The opening in a lock designed to receive the key.
key-in-knob lock A lock with the key cylinder and the other lock mechanism, such as a push or turn button, contained in the knobs.
key plate A plate or escutcheon having only a keyhole.
keyway The longitudinal cut in the cylinder core with an opening or space with millings in the sides identical to those on the proper key, thus allowing the key to enter the full distance of the blade. See also *warded lock*.
knifing See *loiding*.
knob An ornamental or functional round handle on a door; may be designed to actuate a lock or latch.
knob latch A securing device with a spring bolt operated by a knob only.
knob shank The projecting stem of a knob into which the spindle is fastened.
knocked down (KD) Disassembled; designed for assembly at the point of use.
knuckle The enlarged part of a hinge into which the pin is inserted.
laminate A product made by bonding together two or more layers of material.
laminated glass A type of glass fabricated from two layers of glass with a transparent bonding layer between them. Also called *safety glass*.
laminated padlock A padlock, the body of which consists of a number of flat plates, all or most of which are of the same contour, superimposed and riveted or brazed together. Holes in the plates provide spaces for the lock mechanism and the ends of the shackle.
latch (or latch bolt) A beveled, spring-actuated bolt which may or may not include a deadlocking feature.
leading edge See *lock edge*.
leaf, door An individual door, used singly or in multiples.
leaf hinge The most common type of hinge, characterized by two flat metal plates or leaves, which pivots about a metal hinge pin. A leaf hinge can be surface mounted or installed in a mortise. See also *butt hinge* and *surface hinge*.
lever handle A bar-like grip that is rotated in a vertical plane about a horizontal axis at one of its ends; designed to operate a latch.
lever lock A key-operated lock that incorporates one or more lever tumblers, which must be raised to a specific level so that the fence of the bolt is aligned with the gate of the tumbler in order to withdraw the bolt. Lever locks are commonly used in storage lockers and safety deposit boxes.
lever tumbler A flat metal arm, pivoted on one end with a gate in the opposite end. The top edge is spring-loaded. The biting of the key rotates against the bottom edge, raising the lever tumbler to align the gate with the bolt fence. Both the position of the gate and the curvature of the bottom edge of the lever tumbler can be varied to establish the key code.
light A space in a window or door for a single pane of glazing. Also, a pane of glass or other glazing material.
lintel A horizontal structural member that supports the load over an opening such as a door or window.
lip (of a strike) The curved projecting part of a strike plate that guides the spring bolt to the latch point.
lobby That portion of the interior common area of a building that is reached from an entry door and provides access to the general circulation areas, elevators, and fire stairs and from these to other areas of the building.
lock A fastener that secures a door or window assembly against unauthorized entry. A door lock is usually key-operated and includes the keyed device (cylinder or combination), bolt, strike plate, knobs or levers, trim items, etc. A window lock is usually hand-operated rather than key-operated.

lock clip A flexible metal part attached to the inside of a door face to position a mortise lock.
lock edge The vertical edge or stile of a door in which a lock may be installed. Also called the *leading edge*, the *lock stile*, and *strike edge*.
lock edge door (or lock seam door) A door that has its face sheets secured in place by an exposed mechanical interlock seam on each of its two vertical edges. See also *lock seam*.
lock face plate See *face plate*.
locking dog (of a padlock) The part of a padlock mechanism that engages the shackle and holds it in the locked position.
lock-in-knob See *key-in-knob lock*.
lockpick A tool or instrument, other than the specifically designed key, made for the purpose of manipulating a lock into a locked or unlocked condition.
lock rail The horizontal member of a door intended to receive the lock case.
lock reinforcement A reinforcing plate attached inside of the lock stile of a door to receive a lock.
lock seam A joint in sheet metal work, formed by doubly folding the edges of adjoining sheets in such a manner that they interlock.
lock set See *lock*.
lock stile See *lock edge*.
loiding A burglary attack method in which a thin, flat, flexible object such as a stiff piece of plastic is inserted between the strike and the latch bolt to depress the latch bolt and release it from the strike. The loiding of windows is accomplished by inserting a thin stiff object between the meeting rails or stiles to move the latch to the open position, or by inserting a thin stiff wire through openings between the stile or rail and the frame to manipulate the sash operator of pivoting windows. Derived from the word "celluloid." Also called *knifing* and *slip-knifing*.
loose joint hinge A hinge with two knuckles. The pin is fastened permanently to one and the other contains the pinhole. The two parts of the hinge can be disengaged by lifting.
loose pin hinge A hinge with a removable pin that permits the two leaves of the hinge to be separated.
louver An opening with a series of horizontal slats arranged to permit ventilation but to exclude rain, sunlight, or vision.
louvered window A type of window in which the glazing consists of parallel, horizontal, movable glass slats. Also called a *jalousie window*.
main entry door The most important common entry door in a building, which provides access to the building's lobby.
maison keying A specialized keying system, used in apartment houses and other large complexes, that enables all individual unit keys to operate common-use locks such as main entry, laundry room, etc.
masonry Stone, brick, concrete, hollow tiles, concrete blocks, or other similar materials, bonded together with mortar to form a wall, pier, buttress, or similar member.
master disc tumbler A disc tumbler that will operate with a master key in addition to its own change key.
master key system A method of keying locks that allows a single key to operate multiple locks, each of which will also operate with an individual change key. Several levels of master keying are possible: a single master key is one which will operate all locks of a group of locks with individual change keys, a grand master key will operate all locks of two or more master key systems, and a great grand master key will operate all locks of two or more grand master key systems. Master key systems are used primarily with pin and disc tumbler locks and, to a limited extent, with lever or warded locks.
master pin A segmented pin used to enable a pin tumbler to be operated by more than one key cut.
meeting stile The vertical edge member of a door or horizontal sliding window, in a pair of doors or windows, which meets with adjacent edge member when closed. See also *checkrails*.
metal-mesh grille A grille of expanded metal or welded metal wires permanently installed across a window or other opening in order to prevent entry through the opening.
mill finish The original surface finish produced on a metal mill product by cold rolling, extruding, or drawing.
millwork Generally, all building components made of finished wood and manufactured in millwork plants and planing mills. It includes such items as inside and outside doors, window and door frames, cabinets, porch-work, mantels, panelwork, stairways, moldings, and

interior trim. It normally does not include flooring, ceiling, or siding.

molding A wood strip used for decorative purposes.

mono lock See *preassembled lock*.

mortise A rectangular cavity made to receive a lock or other hardware; also, the act of making such a cavity.

mortise bolt A bolt designed to be installed in a mortise rather than on the surface. The bolt is operated by a knob, lever, or equivalent.

mortise cylinder See *cylinder*.

mortise lock A lock designed for installation in a mortise, as distinguished from a bored lock and a rim lock.

mullion (1) A movable or fixed center post used on double door openings, usually for locking purposes. (2) A vertical or horizontal bar or divider in a frame between windows, doors, or other openings.

multiple dwelling A building or portion of a building designed or used for occupancy by three or more tenants or families living independently of each other (includes hotels and motels).

muntin A small member that divides the glass or openings of sash or doors.

mushroom tumbler A type of tumbler used in pin tumbler locks to add security against picking. The diameter of the driver pin behind the end in contact with the bottom pin is reduced so that the mushroom head will catch the edge of the cylinder body at the shear line when it is at a slight to its cavity. See also *spool tumbler*.

night latch An auxiliary lock with a spring latch bolt that functions independently of the regular lock of the door.

nonremovable hinge pin A type of hinge pin that has been constructed or modified to make its removal from the hinge difficult or impossible.

offset pivot (or hinge) A pin-and-socket hardware device with a single bearing contact, by means of which a door is suspended in its frame and allowed to swing about an axis, which normally is located about 1.9 cm (¾″) out from the door face.

one-way screw A screw specifically designed to resist being removed, once installed. See also *tamper-resistant hardware*.

opening size See *door opening*.

operator (of a window sash) The mechanism, including a crank handle and gear box, attached to an operating arm or arms for the purpose of opening and closing a window. Usually found on casement and awning type windows.

overhead door A door that is stored overhead when in the open position.

padlock A detachable and portable lock with a hinged or sliding shackle or bolt, normally used with a hasp and eye or staple system.

panel door A door fabricated from one or more panels surrounded by and held in position by rails and stiles.

panic bar See *crash bar*.

panic hardware An exterior locking mechanism that is always operable from inside the building by pressure on a crash bar or lever.

patio-type sliding door A sliding door that is essentially a single, large transparent panel in a frame (a type commonly used to give access to patios or yards of private dwellings); "single" doors have one fixed and one movable panel; "double" doors have two movable panels.

peeling See *jamb peeling*.

picking See *lockpick*.

pin (of a hinge) The metal rod that serves as the axis of a hinge, thereby allowing the hinge (and attached door or window) to rotate between the open and closed positions.

pin tumbler One of the essential, distinguishing components of a pin tumbler lock cylinder, more precisely called a *bottom pin*, *master pin*, or *driver pin*. The pin tumblers, used in varying lengths and arrangements, determine the combination of the cylinder. See also *bottom pin*, *driver pin*, and *master pin*.

pin tumbler lock cylinder A lock cylinder employing metal pins (tumblers) to prevent the rotation of the core until the correct key is inserted into the keyway. Small coil compression springs hold the pins in the locked position until the key is inserted.

pivoted door A door hung on pivots rather than hinges.

pivoted window A window that opens by pivoting about a horizontal or vertical axis.

plug retainer The part often fixed to the rear of the core in a lock cylinder to retain or hold the core firmly in the cylinder.

preassembled lock A lock that has all the parts assembled into a unit at the factory and, when

installed in a rectangular section cut out of the door at the lock edge, requires little or no assembly. Also called *integral* lock, *mono* lock, and *unit* lock.

pressed padlock A padlock whose outer case is pressed into shape from sheet metal and then riveted together.

pressure-locked grating A grating in which the cross bars are mechanically locked to the bearing bars at their intersections by deforming or swaging the metal.

privacy lock A lock, usually for an interior door, secured by a button, thumb-turn, etc., and not designed for key operation.

projection See *bolt projection*.

push key A key that operates the Ace type of lock.

quadrant See *Dutch door bolt*.

rabbet A cut, slot, or groove made on the edge or surface of a board to receive the end or edge of another piece of wood made to fit it.

rabbeted jamb A door jamb in which the projection portion of the jamb that forms the door stop is part of the same piece as the rest of the jamb or securely set into a deep groove in the jamb.

rail A horizontal framing member of a door or window sash that extends the full width between the sites.

removable mullion A mullion separating two adjacent door openings that is required for the normal operation of the doors but is designed to permit its temporary removal.

restricted keyway A special keyway and key blank for high-security locks, with a configuration that is not freely available and which must be specifically requested from the manufacturer.

reversible local A lock that may be used for either hand of a door.

rim cylinder A pin or disc tumbler cylinder used with a rim lock.

rim hardware Hardware designed to be installed on the surface of a door or window.

rim latch A latch installed on the surface of a door.

rim lock A lock designed to be mounted on the surface of a door.

rose The part of a lock that functions as an ornament or bearing surface for a knob, and is normally placed against the surface of the door.

rotary interlocking dead bolt lock A type of rim lock in which the extended dead bolt is rotated to engage with the strike.

rough buck A subframe, usually made of wood or steel, which is set in a wall opening and to which the frame is attached.

rough opening The wall opening into which a frame is to be installed. Usually, the rough opening is measured inside the rough buck.

sash A frame containing one or more lights.

sash fast A fastener attached to the meeting rails of a window.

sash lock A sash fast with a locking device controlled by a key.

screwless knob A knob attached to a spindle by means of a special wrench, as distinguished from the more commonly used side-screw knob.

screwless rose A rose with a concealed method of attachment.

seamless door A door having no visible seams on its faces or edges.

secondary lock See *auxiliary lock*.

security glass (or glazing) See *burglar-resistant glazing*.

setback See *backset*.

shackle The hinged or sliding part of a padlock that does the fastening.

shear line The joint between the shell and the core of a lock cylinder; the line at which the pins or discs of a lock cylinder must be aligned in order to permit rotation of the core.

sheathing The structural exterior covering, usually wood boards or plywood, used over the framing studs and rafters of a structure.

shell A lock cylinder, exclusive of the core. Also called *housing*.

shutter A movable screen or cover used to protect an opening, especially a window.

side light A fixed light located adjacent to a door within the same frame assembly.

signal sash fastener A sash-fastening device designed to lock windows that are beyond reach from the floor. It has a ring for a sash pole hook. When locked, the ring lever is down; when the ring lever is up, it signals by its upright position that the window is unlocked.

sill The lower horizontal member of a door or window opening.

single-acting door A door mounted to swing to only one side of the plane of its frame.

skylight A glazed opening located in the roof of a building.

slide bolt A simple lock that is operated directly by hand without using a key, a turnpiece, or

other actuating mechanism, Slide bolts can normally only be operated from the inside.

sliding door Any door that slides open sideways.

sliding metal gate An assembly of metal bars that is jointed so it can be moved to and locked in position across a window or other opening in order to prevent unauthorized entry through the opening.

slip-knifing See *loiding*.

solid-core door A door constructed so that the space (core) between the two facing sheets is completely filled with wood blocks or other rigid material.

spindle The shaft that fits into the shank of a door knob or handle. Also serves as its axis of rotation.

split astragal A two-piece astragal, one piece of which is surface mounted on each door of a double door and is provided with a means of adjustment to mate with the other piece and provide a seal. See also *astragal*.

spool tumbler A type of tumbler used in pin tumbler locks to add security against picking. Operates on the same principle as the mushroom tumbler.

spring bolt See *latch*.

spring bolt with antiloiding device See *deadlatch*.

stile One of the vertical edge members of a paneled door or window sash.

stool A flat molding fitted over the windowsill between the jambs and contacting the bottom rail of the lower sash.

stop (of a door or window frame) The projecting part of a door or window frame against which a swinging door or window closes, or in which a sliding door or window moves.

stop (of a lock) A button or other device that serves to lock and unlock a latch bolt against actuation by the outside knob or thumb piece. Another type holds the bolt retracted.

stop side That face of a door that contacts the door stop.

storefront sash An assembly of light metal members forming a continuous frame for a fixed glass storefront.

storm sash, window, or **door** An extra window or door, usually placed on the outside of an existing one as additional protection against cold or hot weather.

strap hinge A surface hinge of which one or both leaves are of considerable length.

strike A metal plate attached to or mortised into a door jamb to receive and hold a projected latch bolt and/or dead bolt in order to secure the door to the jamb.

strike, box See *box strike*.

strike, dustproof A strike placed in the threshold or sill of an opening or in the floor that receives a flush bolt and is equipped with a spring-loaded follower to cover the recess and keep out dirt.

strike, interlocking A strike that receives and holds a vertical, rotary, or hook dead bolt.

strike plate See *strike*.

strike reinforcement A metal plate attached to a door or frame to receive a strike.

strike, roller A strike for latch bolts with a roller mounted on the lip to reduce friction.

stud A slender wood or metal post used as a supporting element in a wall or partition.

stud anchor A device used to secure a stud to the floor.

subbuck (or subframe) See *rough buck*.

surface hinge A hinge having both leaves attached to the surface and thus fully visible.

swing See *hand*.

swinging bolt A bolt that is hinged to a lock front and is projected and retracted with a swinging rather than a sliding action. Also called *hinged* or *pivot bolt*.

tail piece The unit on the core of a cylinder lock that actuates the bolt or latch.

tamper-resistant hardware Builders' hardware with screws or nut-and-bolt connections that are hidden or cannot be removed with conventional tools.

template A precise detailed pattern used as a guide in the mortising, drilling, etc., of a door or frame to receive hardware.

template hardware Hardware manufactured within template tolerances.

tension wrench An instrument used in picking a lock. It is used to apply torsion to the cylinder core.

three-point lock A locking device required on "A-label" fire double doors to lock the active door at three points—the normal position plus top and bottom.

threshold A wood or metal plate forming the bottom of a doorway.

throw See *bolt projection*.

thumb piece (of a door handle) The small pivoted part above the grip of a door handle, which is pressed by the thumb to operate a latch bolt.
thumb turn A unit that is gripped between the thumb and forefinger and turned to project or retract a bolt.
tolerance The permissible deviation from a nominal or specified dimension or value.
transom An opening window immediately above a door.
transom bar The horizontal frame member that separates the door opening from the transom.
transom catch A latch bolt fastener on a transom that has a ring by which the latch bolt is retracted.
transom chain A short chain used to limit the opening of a transom; usually provided with a plate at each end for attachment.
transom lift A device attached to a door frame and transom by means of which the transom may be opened or closed.
trim hardware See *finish builders' hardware*.
tryout keys A set of keys including many commonly used bitings. They are used one at a time in an attempt to unlock a door.
tumbler A movable obstruction in a lock that must be adjusted to a particular position, as by a key, before the bolt can be thrown.
turn piece See *thumb turn*.
unit lock See *preassembled lock*.
vertical bolt lock A lock with two dead bolts that move vertically into two circular receivers in the strike portion of the lock attached to the door jamb.
vision panel A fixed transparent panel of glazing material set into an otherwise opaque wall, partition, or door; a nonopening window. See also *light*.
ward An obstruction that prevents the wrong key from entering or turning in a lock.
warded lock A lock containing internal obstacles that block the entrance or rotation of all but the correct key.
weather-stripping Narrow or jamb-width sections of flexible material that prevent the passage of air and moisture around windows and doors. Compression weather-stripping also acts as frictional counterbalance in double-hung windows.
wet glazing The sealing of glass or other transparent material in a frame by the use of a glazing compound or sealant.
window frame See *frame*.
window guard A strong metal grid-like assembly that can be installed on a window or other opening; types of window guards include metal bars, metal-mesh grilles, and sliding metal gates.
wire glass Glass manufactured with a layer of wire mesh approximately in the center of the sheet.

CHAPTER

8

Safes, Vaults, and Accessories

Kenneth Dunckel, Gion Green

CHOOSE THE RIGHT CONTAINER

A safe or vault ideally should occupy the innermost ring of concentric *protective rings* around a secured premise. Other security equipment (fences, gates, vehicle barriers, doors, and access controls) selected for the outer protective rings is usually specifically designed for its function, but the security vault at the center often is not.

The value and physical nature of a vault container's contents should dictate the type of container and degree of protection sought; but people tend to categorize all combination-locked security containers as "safes" because of one common denominator—combination locks. This is a mistake.

There are fire-resistant safes, burglary-resistant chests, safes for EDP media, and insulated filing cabinets. Each can be combination locked, but to regard any combination-locked container as a safe is to disregard the fact that different types and levels of protection exist. Such disregard invites losses.

High-value items stored in a fire-resistant safe or insulated filing cabinet are vulnerable to burglary—the average insulated container can quickly be forced open with a few simple, accessible hand tools. Similarly, important documents stored in a burglary chest are much more secure from burglars than in an insulated container, but are also more likely to be incinerated in a fire.

Underwriters Laboratories (UL) systematically tests the fire- and burglary-resistant qualities of representative security containers submitted by their manufacturers (see Appendix 8.A). Makers of those containers that meet specific test requirements may affix a UL rating label to their products. The presence of a UL label signifies that a comparable unit of the same design successfully passed systematic tests performed by UL for resistance to burglary or fire. The label denotes the type and severity of test conditions.

Possibly the best protection are those safes that bears UL labeling for both fire and burglary protection. Such containers are simply burglary chests housed inside insulated containers. Similar protection can be obtained by buying a burglary chest and a fire safe separately, then placing the burglary-resistant chest inside the fire safe, thus establishing separate storage areas for documents and high-value items.

Because UL ratings are recognized by the American insurance industry as reliable rating standards for security containers, comprehensive insurance policies often specify or otherwise require minimum UL security container ratings. Reduced mercantile insurance rates may be applicable if a selected security container has the recommended minimum rating.

Whether or not a security container provides fire or burglary protection, its inherent security can be increased with special-function locks. Very often, the purchaser of a fire safe or money chest is not told of all the optional equipment available with the security container being considered. Salespeople often prefer not to risk confusing their clients with too many options. Optional equipment boosts the sale price and thus can jeopardize a sale. People who buy security containers should nevertheless be aware of what is available and decide for themselves. If unwisely chosen, the security container can cause new operational and logistical problems, which could be solved by the use of special-function equipment.

For instance, the presence of a quality burglary-resistant chest on the premises of a cash-handling business means that a bank deposit does not necessarily have to be made daily, even if daily deposits are supposed to be the usual procedure. An attitude of "nothing to worry about—just put it in the safe overnight" can easily develop. But an after-hours visit by a dishonest employee with the combination can double the loss potential. So, too, can a properly timed holdup. The situations that can be prevented or alleviated by wisely chosen security equipment are numerous, and safe buyers should be aware of them. The following sections describe a few such possibilities and the security equipment that is presently available for prevention.

UL-RATED COMBINATION LOCKS

A good quality combination lock is a basic need. On well-made containers, the most common combination locks are those certified in accordance with UL standards (UL 768). Combination locks can earn a Group 1, 1R, or 2 classification. A lock bearing a UL label has met or exceeded detailed criteria for quality, security, and durability.

The UL testing procedure for combination locks involves ascertaining that the lock can be set to various combinations and operated within specified tolerances. According to Section 11.10 of UL 768:

> *A three-tumbler wheel lock shall not open with the dial turned more than 1½ dial gradations on either side of the proper gradation for each tumbler. A four-tumbler lock shall not open with the dial turned more than 1½ dial gradations on either side of the proper gradation for each number.*

Other sections of UL 768 describe tests for mechanical strength, impact resistance, manufacturing tolerance, product endurance, and operability after prolonged exposure to adverse conditions. The testing for UL Group 1 (manipulation resistant) and Group 1R (manipulation and radiographic resistant) labels includes all tests performed on Group 2-rated locks plus the requirement that the lock tested must, by virtue of its design and construction, resist skilled surreptitious attempts to learn the combination numbers by manipulation, the use of instruments, or radioactive isotopes (Group 1R test only) for 20 worker-hours of net working time.

In most instances, a Group 2 combination lock provides adequate security. Although many legitimate safe and vault technicians are trained in combination lock manipulation techniques, criminals with the skill and knowledge necessary to surreptitiously open a Group 2 lock by manipulation are few in number. Most safe burglars use forceful methods. High-security installations, however, such as jewelry safes or containers protecting extremely sensitive or classified information, should be outfitted with manipulation-resistant Group 1 locks to block every possible avenue of criminal approach.

Defense contractors who deal with classified information are required to protect such information in security containers that meet certain government specifications. One such specification, MIL-L-15596, defines the type of combination lock that is acceptable. This specification covers much the same territory as the UL standard regarding Group 1 and 1R manipulation- and radiation-resistant locks.

RELOCKING DEVICES

A relocking device, or relocker, is an auxiliary bolt or bolt-blocking mechanism for which there is no control from outside the container. Relockers protect security containers against torch, drill, and punching attacks. The relocker is an especially important feature on burglary-resistant units, because these containers are designed to protect items of high dollar value and are therefore more attractive to skilled burglars. Relockers are important enough in preserving a container's security to warrant a separate standard for rating them, UL 140.

Known in bygone days as *dynamite triggers*, relockers can be simple in design; often they are no more than spring-driven bolts held in a cocked (loaded) position until activated by a burglar's attack. With normal usage of a relock-equipped container, the relocker's presence is undetectable to the user. When activated, the relocker blocks the retraction of the door bolts, combination bolt, or both, even if the correct combination for the lock is known.

Relocking devices are often held cocked by a piece of metal attached by screws to the combination lock's back cover. When thus situated, relockers protect against spindle or dial punching, the most common (and in earlier times one of the most effective) forms of forceful burglary attack.

In a typical punching attack the burglar first knocks the dial off the safe to expose the end of the spindle, a threaded shaft that connects the numbered safe dial to the combination lock's wheels. The spindle end is then punched inward with a hand sledge and drift punch. When the spindle is driven inward in this manner, one or more of the lock's wheels are slammed against or even through the back cover of the lock. A punching attack may completely dislodge all the wheels (or tumblers) in the lock.

Most currently manufactured combination lock back covers are purposely designed to be dislodged by a punching attack. Because the relock checking device is fastened to the lock cover or located very near it, dislodging the cover also dislodges the relock check. A spring (or in some cases gravity) then takes over, moving the relock to its triggered position.

After spindle punching, the burglar can insert tools through the spindle hole and fish the combination bolt to a retracted position. If not for relockers the safe door could be opened. A triggered relocker, however, is not easily located or easily released from outside the container. Containers incorporating some form of relocking device now outnumber older, non-relock-equipped containers; an unsuccessful punching attempt on a recently built container signifies a lack of knowledge and skill.

Although makers of fire-resistant containers are not required to include a relocking device in the container design, many do so to thwart the type of punching attack just described. Safe makers realize that, because the cost per cubic inch of space in a fire-resistant container is appreciably less than that of a burglary-resistant container of the same size, many clients store high-value items in fire-resistant containers instead of burglary chests, even after being advised not to.

Thermal relocking devices hinder skilled burglars who use cutting torches or other burning tools. A thermal relock activates when the part of the mechanism that holds the relock cocked (usually a fusible link made from a metal with an extremely low melting point) heats to its melting point, at which time a spring can activate a bolt-blocking mechanism. A thermal relock is not necessarily part of the combination lock but is usually nearby, because torching burglars tend to burn in an area fairly close to the combination lock.

Current Group 1, 1R, and 2 combination locks have simple but effective built-in relocking devices designed to be activated by spindle-punching attacks. Some also incorporate thermal protection. Many safe makers, however, do not rely totally on the protection provided by these built-in relockers, preferring to include relockers of their own design, situated outside the combination lock.

Some safe makers use a sophisticated type of relocking device that simultaneously guards

against punching, drilling, and burning attacks. A *nerve plate* of tempered glass is mounted between the combination lock and the inner surface of the container door. Taut wires or cords are strung from one or more spring-driven relocking devices and fastened to the glass. The placement of such nerve plates ensures that most unskilled and semi-skilled burglary attacks will severely shock and thus shatter the glass nerve plate. Similarly, a skilled operator who attempts to drill into the lock case and manipulate the combination wheels will encounter the nerve plate before penetrating the lock. Any attempt to penetrate further will shatter the glass and release the tension on the wires that hold the relocks cocked.

Glass nerve plates have been popular with foreign safe makers for some time. They are an extremely efficient way to hinder even highly skilled burglars. Some makers of high-security units string the relock wires around a series of posts before attaching them to the nerve plate in front of the combination lock. Relockers and the wires can be placed randomly within a production run of like models, defeating those burglars armed with blueprints made by taking exact measurements from a comparable model.

UL tests and certifies relocking devices under the standard UL 140. Safe makers whose relocking devices are successfully tested under the conditions described in UL 140 are entitled to affix labels to that effect on their containers.

LOCKING DIALS

Locking combination dials are used to ensure that no one person has control of a security container's contents. Companies whose employees handle large amounts of cash or other valuables use locking dials to satisfy dual custody requirements. Typically, one person is assigned the key that unlocks the dial and another is assigned the combination. A locked dial will not turn to allow the combination to be dialed until the keyholder unlocks it. The keyholder can lock or unlock the dial but cannot open the container without the combination.

A typical application of dual custody is for a supermarket safe. Usually, notice is posted to the effect that two people are required to open the safe; the store manager has only the combination, and the armored car guard has the dial key. When this procedure is used, such arrangements deter or complicate holdups.

When used according to strictly observed procedures, locking dials also help reduce the opportunity for a lone dishonest person to abuse a position of trust and can help protect innocent persons from unwarranted suspicion when mysterious losses are noted.

LOCKABLE HANDLES

Lockable bolt control handles perform much the same function as lockable dials. A locking handle allows the combination to be dialed, but the bolt control handle does not retract the door bolts until it is unlocked. Again, this arrangement allows dual custody of the container's contents.

Users of walk-in vaults often leave the combination dialed and the door bolts retracted during business hours. Hold-up gangs have used this fact to their advantage by herding their victims into the vault and then simply turning the bolt handle and spinning the combination dial to lock them in to ensure a clean getaway. When installed on the door of a walk-in vault, locking bolt control handles helps to prevent this tactic, because the door bolts can be immobilized during the business day.

TIME LOCKS

Time locks are considered standard equipment on bank vault doors but may also be used on any security container whose door has enough usable surface area to permit installation. A time lock ensures that, once closed and locked, the safe or vault door remains so for a predetermined amount of time. Time locks were hailed by nineteenth century bankers as devices that would discourage the kidnapping of bank officials and their family members to force disclosure of vault combinations. Before time locks, this was

a common tactic of holdup and burglary gangs who did not balk at committing brutal crimes to learn vault combinations.

The most common time locks are mechanical windup mechanisms; their internal design and operation is quite similar to that of ordinary timepieces, but their mainsprings perform additional duties besides powering the clockworks.

When a mechanical time lock is wound, a shutter in its case closes. Usually, a rod or projection extends from the door bolts; when the bolts move, the rod moves. During bolt retraction (i.e., opening the safe door), this rod would normally enter the time lock case via the shutter hole, but the closed shutter blocks the rod's passage, which translates to a door bolt blockage. As the time lock's movements wind down, the mainspring's energy is harnessed to open the shutter. The shutter reopens fully when the first movement has wound down.

A typical time lock relies on at least two, but as many as three or four, separate windup movements in a single case. It can be used on safes as well as vaults. The presence of at least two movements gives reasonable assurance that a single movement's failure does not cause a lockout; the more movements used, the more the chance for lockout is reduced. Only one movement must wind down for the container to open.

TIME-DELAY COMBINATION LOCKS

No lock can prevent an armed robber from forcing another person to disclose a combination. This type of robbery is often committed against restaurant or store employees in the hours before or after closing. Such crimes often net rich hauls for criminals and can easily involve injury to the victims.

The robbers gain entry to the premises by various methods: by capturing an employee while entering or exiting, by using a seemingly legitimate pretext, or sometimes by breaking into the premises and lying in wait for the holder of the safe combination. Once identified, that person is forced to open the safe.

Time-delay combination locks, also known as *delayed action timers* (DATs), are one solution to the problem, because such locks can foil or deter robberies. A time-delay lock is a combination lock with one or more timer movements attached. The action of dialing the safe combination winds a timer. The operator must wait for a predetermined period after dialing before the delay mechanism permits the combination lock bolt to retract. Delay times range from as few as 3 minutes to as many as 45 minutes and in some cases are changeable.

The most sophisticated time-delay combination locks boast alarm compatibility. A store manager ordered by a robber to open the safe can discreetly dial a special combination and activate a holdup alarm. Alarm-compatible time-delay combination locks give police a better chance of arriving in time to make an arrest.

Time-delay locks reduce both robbery losses and the incidence of robbery. Businesses using time-delay locks usually post conspicuous notices to this effect, causing prospective robbers to take their business elsewhere. Robbers rely on speed of execution—even the hint of a delay reduces a target's appeal.

ALARMED COMBINATION LOCKS

Alarmed combination locks incorporate microswitches capable of shunting alarms and signaling unauthorized opening attempts or openings made under duress.

Perhaps the most generally useful are the switches designed to send *duress* alarm signals. They are designed to discreetly send an alarm signal when a special duress combination is dialed. Like the regularly used combination, the duress combination also opens the safe, so that a robber does not realize an alarm is being sent.

The typical robber orders the victim not to set off an alarm, and things can get ugly if the robber suspects otherwise. Because the alarm is set off by a seemingly innocent dialing procedure performed in accord with the robber's demands, combination locks with duress or ambush features could be categorized as compliance alarms.

Tamper switches help protect combination-locked containers during those hours when no persons, not even authorized combination holders, are allowed access to the contents. The dial is set at a predetermined number and sometimes locked in place, and then the alarm protection is turned on. Any attempt to dial the combination while the protection is on causes an alarm.

Another switch arrangement can be used to monitor the status of the container or as an alarm shunt. This switch is placed in such a way that, when the combination lock bolt is retracted to the open position, the switch is actuated. This lets remote monitors track the container's openings and closings. A shunt switch allows the burglary alarm circuit to remain active 24 hours a day while still allowing combination holders access to the contents.

VISION-RESTRICTING AND SHIELDED DIALS

Standard combination dials are known as *front-reading*, meaning that their numbers are visible from a horizontal line of sight. It is possible for prying eyes to see the numbers that are dialed when a front-reading dial is used, which of course makes the safe's protection ineffective. If a combination must be dialed while persons not authorized to know the numbers are nearby, a front-reading dial is best replaced with a vision-restricting, or *spyproof*, dial.

Various types of vision-restricting dials are available, and each safe lock manufacturer has its own version. One of the most common is the top-reading dial, whose numbers are etched into an outer rim perpendicular to the safe door. To effectively see the combination numbers, the dialer must stand squarely in front of the dial and look down at the numbers while dialing. A raised flange guards the sides of the dial from view; only a small portion of the dial's numbered area can be seen at any given time.

Other vision-restricting designs incorporate covered dials with louvered windows or tinted and polarized lenses at the index area. Covering the entire dial except the turning knob shields the dial face from finger marks. People who dial safe combinations tend to place one finger on the dial face as a brake. This leaves smudges on the safe dial at fairly regular distances from the actual combination numbers, thus making it possible to learn a safe's combination by composing test combinations as suggested by the smudges' locations.

COMBINATION CHANGING

A positive aspect of combination locks is user changeability. Although many companies leave this task to service vendors as a matter of policy, some have policies dictating that company personnel do the changing to absolutely ensure exclusive knowledge of combination numbers. New safes, chests, and insulated files, if combination locked, usually come with detailed instructions for changing and special change keys.

Safe dealers often remove the changing instructions and changing keys before delivery, and with good reason. The customer's first suspicion might be that the safe dealer would much rather profit from future service calls to change combinations than let the clients do it themselves. This is partly true, but there is a valid reason for withholding changing tools and instructions.

Safe buyers who have changing instructions and try to change keys often fall victim to a common syndrome. They attempt combination changes before having fully read or understood the instructions and thus cause a lockout.

The client calls the dealer for help, and, because the lockout is attributable to error rather than a defective product, is charged for the work. Not wishing to pay a service fee, the client does not admit the error, claiming instead that the unit is defective and that the work should be covered by warranty. The dealer's representative knows better: combination-changing errors are glaringly obvious to a technically experienced person. The dealer's subsequent refusal to write the work off as a warranty job incurs the client's wrath and creates bad will.

Combination changing is a relatively simple task, but mistakes can be costly in terms of

both lost time and dollars. Safes are unforgiving—a lockout resulting from a combination-changing error may dictate that the container be forced open. Lockouts can be avoided by exercising a high degree of care when working with the combination lock components and always trying new combinations several times with the safe door open. This is probably the most important yet most ignored part of combination changing.

SAFE BURGLARIES

At a time in the not-so-distant past, gangs of skilled safe burglars operated in America; pickings were easy and plentiful. In today's world, where the need for instant gratification often supersedes reason, fewer criminals spend the time necessary to learn safe burglary skills and properly plan and execute safe burglaries. Contemporary criminals tend to prefer crimes that require much less time or technical skill; a fast exchange of drugs and money in a motel parking lot can easily net more than a weekend of work with a cutting torch.

Highly skilled, knowledgeable safecrackers are by no means extinct in America, but there are a lot fewer of them today. The remaining safecrackers with sufficient skill to breach a well-built jeweler's chest or bank vault do not need to work as often as other thieves; consequently, their exploits do not get the continual press coverage that more prolific criminals receive.

The burglar most likely to visit a business or residential premises is fairly average in terms of technical skill. Such individuals work fast and often. While very good at defeating or circumventing door and window locks, this type of burglar is usually stumped when confronted by even a thin-walled insulated safe—quite often his or her best effort will be an unsuccessful attempt at prying or dial punching, after which the container may be locked more securely than before. In addition to technical ignorance, the would-be safecracker usually suffers from a faint heart and would rather leave than invest much time in the effort.

Some burglars, however, inhabit a middle ground with respect to skill. They have learned to recognize and prepare for those situations in which they have a fair chance of getting into some of the safes they may encounter. These individuals find enough opportunities and enjoy enough success within the parameters of their limited skills that they usually do not make the effort to become more technically proficient. They pose a real threat, because part of their expertise is in the exploitation of human error and complacency, failings to which even users of high-security containers are subject.

The only defense against the semi-skilled opportunistic safe burglar is knowledge, awareness, and strict adherence to proper security procedures. The following are some of the ways these individuals gain access to safe contents and suggestions for defeating them.

HIDDEN COMBINATIONS

Many people, fearful of forgetting the safe combination, write down the numbers and dialing sequences and hide them somewhere near the safe or in a wallet or address book. Smart burglars know more places to look for combination numbers than the average person can dream of and systematically search for and discover them, no matter how well hidden the safe user may think they are. Combination numbers can be memorized, a fact that makes combination locks more secure than the majority of key-operated mechanisms. Writing out the combination is a real help for burglars and can complicate police investigations. Safe users who write down combinations often do so in violation of company security policies. Therefore, they are reluctant to admit it, forcing investigators to guess at the facts. Prevention is simple: Memorize the numbers.

Using Birthdays, Phone Numbers, Addresses, and the Like

Such numbers are appealing because they are already committed to the user's memory, but

smart burglars have been known to take the time to do some research on their victims, learning the same numbers and composing test combinations with them. Similarly, many safe users tend to select combination numbers ending in 5 or 0, like 10-20-50 or 25-35-15, because such numbers are more clearly marked on the safe dial. Doing so greatly limits the combination possibilities. A safe combination should ideally be a random set of numbers with no special significance to the user.

Failing to Fully Scramble the Combination When Locking

This is especially common in cases where the safe is outfitted with a locking dial. For daytime convenience the combination numbers are left dialed, then the bolt is left extended and the dial locked with the key. The safe door can be opened by merely turning the dial key and moving the dial just a few numbers' worth of travel, rather than having to redial completely. Safe users mistakenly think the dial lock and combination lock afford equal protection, but they do not. The combination lock is protected inside the safe door while the dial lock is exposed on the outside. Safes without locking dials can also be locked but not fully scrambled and thus afford opportunities for patient thieves to walk the dial a number at a time in hope of finding the last number of the combination. Whenever a safe is closed it is a good practice to turn the dial at least four full revolutions before considering it locked.

Smart burglars confronted with a locking dial can sometimes make a big score by merely clamping a heavy pair of pliers on the dial and twisting, because people who hate to dial safe combinations can easily slip into the habit of using the dial lock for nighttime locking as well as daytime convenience. Daytime robbers have also been known to give the same treatment to safes secured only by locking dials during business hours. Simply stated, the dial lock protects the dial, and the combination lock protects the safe.

Punching

The majority of burglary-resistant safes are protected in some way against punching; relocking devices and punch-resistant spindles are the most popular methods. Many insulated safes built in the last 20–30 years also feature relocking devices. Punching is generally a sign of technical ignorance. The safe dial is pried or knocked off and a punch or lineup tool is used in conjunction with a hand sledge to drive the spindle inward. The intent is to knock the lock components completely out of position so they no longer block the retraction of the door bolts. In safes not equipped with relocking devices or other protective measures, punching is usually effective. The best defense against punching attacks is to buy a safe equipped with a UL-listed relocking device.

While protection against burglary is not an absolute necessity in a fire-resistant container, many makers of such containers realize that safe users often treat their products as if they were burglary-resistant chests and store high-value items in them. With this in mind, the safe makers usually include relocking protection of some sort, if only by being certain to use a combination lock with built-in relock protection.

Peeling

Insulated containers can often be peeled open in much the same way as a sardine can. Often the burglar will pound with a sledge near one of the door's corners in an effort to buckle it inward, thus permitting the insertion of wedging and prying tools. The door is then peeled back by virtue of sheer force until the contents can be removed. In another type of peeling attack, a chisel separates the outer metal skin from the door. This outer skin of older fire safes was in many cases merely spot-welded in several locations along the door's edge. When the initial separation has been achieved, a larger chisel (fire axes and heavy prying tools have been used) continues the process of breaking the remaining spot welds all the way down the door's edge, until the outer skin can be bent or peeled out of the way. The intent in such

attacks is to dig or chop through the door insulation and inner skin, eventually exposing the combination lock or door bolts and overcoming them with heavy tools and brute force. More recently made insulated containers have seam-welded door skins to make this type of attack extremely difficult, if not unfeasible. Although fire safes can be peeled by both semi-skilled and skilled criminals, the neatness and efficiency of the work gives an indication of the criminal's skill and experience. A sturdily built money or jewelry chest cannot be peeled.

Ripping or Chopping

These forms of attack are most often successful when carried out against insulated containers. The burglar may be unskilled, semi-skilled, or professional. Heavy metal-cutting tools cut a hole in the container's door, side, or bottom. When the hole is made, the burglar simply reaches in and removes the contents. Defeating the peelers and rippers of the world requires only that the safe purchased be a burglary chest rather than an insulated container. If both fire and burglary protection are necessary, a burglary-resistant container can be installed inside an insulated container.

Carting Off

Also known by burglary investigators as a *kidnap* or *pack-off*, this is the simplest but perhaps the nerviest safe defeat. If the container can be moved and transported easily enough, the burglar or burglars simply steal the entire container and open it at their leisure in a secure location. The majority of existing insulated containers are wheeled, making this task even easier than it should be. Often a bolt-down kit is available, which enables the safe owner to attach the safe to the floor of the premises and hinder burglars who might try stealing it. At the very least, the wheels of a fire safe should be removed after delivery. To protect a smaller burglary-resistant chest, install it inside a box or metal jacket bolted or anchored to the floor and filled with concrete. The concrete jacket adds appreciably to the weight of the unit and severely complicates its unauthorized removal as well as side attacks by skilled and semi-skilled safecrackers.

Skilled Attacks

The skilled safecracker is relatively rare in America, but a few are in business. Their skills and specialties vary, and they have a wide variety of easily available equipment to choose from: high-speed drills, low-rpm/high-torque drills, core-drills, Carborundum cutters, saber saws, cutting torches, oxy-arc lances, burning bars, and explosives. The only way to defeat safe burglars who work with such effective gear is to ensure that the actual attack is time-consuming and fraught with the danger of discovery or capture. The less appealing the target, the more likely the professional is to seek easier pickings.

If there is genuine concern about the possibility of a skilled attack, the first and most obvious thing to do is to buy a burglary-resistant container with a rating equal to or exceeding the recommendation of a knowledgeable insurance agent. Today, safes are designed to put up a staunch fight against even the well-equipped, highly skilled professional safecrackers of the world. A reliable intrusion detection system is necessary; it should protect both the perimeter of the premises and the safe. If the safe is to be used commercially, a security policy should be established and rigorously adhered to. A security policy should define and expressly prohibit breaches of security such as those described earlier (i.e., writing down combination numbers or leaving the combination partially dialed); all such actions should be expressly forbidden.

OVERCOMING SAFE-OPENING PROBLEMS

Safe users often experience difficulty when trying to open a safe. The combination just does not seem to catch when it is dialed. This problem, on the surface, is an operational inconvenience, but there are security implications as well.

Safe users often learn to live with balky safes and combination locks: the money for repair and adjustment just is not in the budget or they may wonder if the difficulty is entirely the safe's fault. Many people hesitate to make an issue of a dialing problem for fear of exhibiting ignorance or inability to perform what, on the surface, is a simple rote task. Consequently, they accept that they must dial and redial to open the safe each day, breathe a sigh of relief when the combination finally takes, and then do something that may constitute a breach of their employers' security policy. Rather than opening the safe, removing what is needed, closing the door, throwing the door bolts, and rescrambling the combination, the irritated safe user leaves the combination dialed to avoid the added irritation of the dial-redial routine several more times during the business day.

This usually works nicely until the day when everybody goes out for lunch and forgets that a turn of the door handle is all that is necessary to open the safe door. A lunchtime office prowler finds it hard to resist trying the safe handle and is rewarded for this small expenditure of energy. The scenario varies, but is generally the same: People who use safes and combination locks often adapt to the inconveniences caused by malfunctioning locks, improper dialing procedures, or maintenance-starved mechanisms by shortchanging their own security procedures.

Another all-too-possible situation, the robbery, presents more grave considerations. The same person who must routinely make several tries at opening the safe is ordered by armed robbers to open the safe immediately, then the criminals interpret fumbling as a delaying tactic and react violently.

These are only a few reasons why it is in the best interest of all concerned to have a properly maintained security container and well-trained users of that container. The following information helps safe users open those balky safes with fewer tries. But, these guidelines should not be interpreted as another set of adaptive measures to forestall necessary maintenance.

- When dialing a safe combination, stand squarely in front of the safe and look directly at the numbers. Viewing them from an angle causes improper dial settings.
- Align the dial numbers exactly with the index mark at the top of the dial.
- Follow the safe maker's dialing instructions exactly. If the safe used has no factory-supplied dialing instructions, contact the factory or a local safe dealer for some. Usually, they will be supplied at no charge.
- Do not spin the dial—this accelerates wear and can cause breakage.

When the safe does not open after the combination has been correctly dialed, a few dialing techniques usually get results. The first is to add one number to each of the combination numbers and dial as if this were the actual combination. For example, if the combination numbers are 20-60-10, try 21-61-41 using the same dialing procedure as usual.

If adding 1 to each of the combination numbers does not help, subtract 1 from each of the actual combination numbers. For example, with an actual combination of 20-60-40, the next combination to try would be 19-59-39. One of these two procedures works surprisingly often.

If neither of these procedures is successful, the next procedure is to progressively add 1 to each setting and dial the other numbers as usual, again using the normal dialing procedure. For example, if the correct combination is 20-60-40, the progression would be to dial 21-60-40, 20-61-40, then 20-60-41. If this procedure is unsuccessful, the next procedure is to progressively subtract from each combination setting. For example, if the original combination is 20-60-40, dial 19-60-40, 20-59-40, and 20-60-39.

These procedures overcome lock wear and dialing errors—users may habitually and unconsciously misalign combination numbers at the dialing index mark. Interpret the success of any of these procedures as a signal that the mechanism needs inspection and service. It is a mistake to simply continue using the safe without correcting the condition that required using a set of numbers

other than those actually set. If the condition that necessitated these dialing procedures was caused by a need for service or adjustment, a future lockout is a strong possibility if service is not obtained.

APPENDIX 8.A. RATING FILES, SAFES, AND VAULTS*

Gion Green

The final line of defense at any facility is at the high-security storage areas where papers, records, plans or cashable instruments, precious metals, or other especially valuable assets are protected. These security containers will be of a size and quantity that the nature of the business dictates.

The choice of the proper security container for specific applications is influenced largely by the value and the vulnerability of the items to be stored in them. Irreplaceable papers or original documents may not have any intrinsic or marketable value, so they may not be a likely target for a thief; but since they do have great value to the owners, they must be protected against fire. On the other hand, uncut precious stones, or even recorded negotiable papers that can be replaced, may not be in danger from fire, but they would surely be attractive to a thief; therefore, they must be protected.

In protecting property, it is essential to recognize that, generally speaking, protective containers are designed to secure against burglary *or* fire. Each type of equipment has a specialized function, and each type provides only minimal protection against the other risk. There are containers designed with a burglary-resistant chest within a fire-resistant container, which are useful in many instances; but these, too, must be evaluated in terms of the mission.

Whatever the equipment, the staff must be educated and reminded of the different roles played by the two types of containers. It is all too common for company personnel to assume that the fire-resistant safe is also burglary-resistant, and vice versa.

*From Fischer, RJ, Green, G. *Introduction to Security*, 6th ed. Boston: Butterworth-Heinemann, 1998.

FILES

Burglary-resistant files are secure against most surreptitious attacks. On the other hand, they can be pried open in less than half an hour if the burglar is permitted to work undisturbed and is not concerned with the noise created in the operation. Such files are suitable for non-negotiable papers or even proprietary information, since these items are normally only targeted by surreptitious assault.

Filing cabinets, with a fire-rating of 1 hour, and further fitted with a combination lock, would probably be suitable for all uses but the storage of government classified documents.

SAFES

Safes are expensive, but if they are selected wisely they can be one of the most important investments in security. Safes are not simply safes. They are each designed to perform a particular job to a particular level of protection. To use fire-resistant safes for the storage of valuables—an all too common practice—is to invite disaster. At the same time, it would be equally careless to use a burglary-resistant safe for the storage of valuable papers or records, because if a fire were to occur, the contents of such a safe would be reduced to ashes.

RATINGS

Safes are rated to describe the degree of protection they afford. Naturally, the more protection provided, the more expensive the safe will be. In selecting the best one for the requirements of the facility, an estimate of the *maximum* exposure of valuables or irreplaceable records will have to be examined along with a realistic appraisal of their vulnerability. Only then can a reasonable permissible capital outlay for their protection be achieved.

Fire-resistant containers are classified according to the maximum internal temperature permitted after exposure to heat for varying periods (Table 8-1). A record safe rated 350-4 (formerly designated "A") can withstand exterior temperatures building to 2,000°F for 4 hours without permitting the interior temperature to rise above 350°F.

TABLE 8-1 Fire-Resistant Containers: UL Record Safe

Class	Resistance to Attack	Attack Time	Description
Fire			
350°F	Not tested	N/A	For paper and document storage
150°F	Not tested	N/A	For storage of magnetic computer tapes and photographic film
125°F	Not tested	N/A	For storage of flexible disks
Burglary			
TL-15	Door and body	15 minutes	Resists against entry by common mechanical and electrical tools
		30 minutes	Door and *entire body* must resist attack with tools and torches listed above plus electric impact hammers and oxy-fuel gas cutting or welding torches
TXTL-60	Tool, torch, and explosive resistant	60 minutes	Weight: At least 1,000 pounds. Door and entire safe body must resist attack with tools and torches listed above plus 8 ounces of nitroglycerine or equal.

UL tests that result in the various classifications are conducted to simulate a major fire with its gradual buildup of heat to 2,000°F and where the safe might fall several stories through the fire-damaged building. Additionally, an explosion test simulates a cold safe dropping into a fire that has already reached 2,000°F.

The actual procedure for the 350-4 rating involves the safe staying 4 hours in a furnace that reaches 2000°F. The furnace is turned off after 4 hours, but the safe remains inside until it is cool. The interior temperature must remain below 350°F during the heating and cooling-out period. This interior temperature is determined by sensors sealed inside the safe in six specified locations to provide a continuous record of the temperatures during the test. Papers are also placed in the safe to simulate records. The explosion impact test is conducted with another safe of the same model that is placed for 30 minutes in a furnace preheated to 2,000°F. If no explosion occurs, the furnace is set at 1,550°F and raised to 1,700°F over a half-hour period. After this hour in the explosion test, the safe is removed and dropped 30 feet onto rubble. The safe is then returned to the furnace and reheated for 1 hour at 1,700°F. The furnace and safe are allowed to cool; the papers inside must be legible and uncharred.

350-2 record safes protect against exposure up to 1,850°F for 2 hours. The explosion/impact tests are conducted at slightly less time and heat. 350-1 gives 1 hour of protection up to 1,700°F and a slightly less vigorous explosion/impact test. Computer media storage classifications are for containers that do not allow the internal temperature to go above 150°F. Insulated vault door classifications are much the same as for safes except that they are not subject to the explosion/impact test.

UL testing for burglary resistance in safes does not include the use of diamond core drills, thermic lance, or other devices yet to be developed by the safecracker.

In some businesses, a combination consisting of a fire-resistant safe with a burglary-resistant safe welded inside may serve as a double protection for different assets, but in no event must the purposes of these two kinds of safes be confused if there is one of each on the premises. Most record safes have combination locks, relocking devices, and hardened steel lock plates to provide a measure of burglar resistance, but it must be reemphasized that record safes are designed to protect documents and other similar flammables against destruction by fire. They provide only slight deterrence to the attack of even unskilled burglars. Similarly, burglar resistance is powerless to protect the contents in a fire of any significance.

CHAPTER

9

Security Lighting

Philip P. Purpura, CPP, Lawrence J. Fennelly, CPO, CSS, HLC III, Gerard Honey, James F. Broder, CPP

Adequate light not only helps people recognize and avoid danger, but also in many cases deters criminals by creating in them the fear of detection, identification and apprehension.

Randy Atlas, CPP (1993)

INTRODUCTION

From a business perspective, lighting can be justified because it improves sales by making a business and merchandise more attractive, promotes safety and prevents lawsuits, improves employee morale and productivity, and enhances the value of real estate. From a security perspective, two major purposes of lighting are *to create a psychological deterrent to intrusion* and *to enable detection*. Good lighting is considered such an effective crime control method that the law, in many locales, requires buildings to maintain adequate lighting.

One way to analyze lighting deficiencies is to go to the building at night and study the possible methods of entry and areas where inadequate lighting aids a burglar. Before the visit, contract local police as a precaution against mistaken identity and recruit their assistance in spotting weak points in lighting.

What lighting level aids an intruder? Most people believe that, under conditions of darkness, a criminal can safely commit a crime. But this view may be faulty, in that one generally cannot work in the dark. Three possible levels of light are bright light, darkness, and dim light. *Bright light* affords an offender plenty of light to work but enables easy observation by others; it deters crime. Without light, in *darkness*, a burglar finds that he or she cannot see to jimmy a good lock, release a latch, or do whatever work is necessary to gain access. However, *dim light* provides just enough light to break and enter while hindering observation by authorities. Support for this view was shown in a study of crimes during full-moon phases when dim light was produced.

This study examined the records of 972 police shifts at three police agencies over a 2-year period to compare nine different crimes during full-moon and non-full-moon phases. Only one crime, breaking and entering, was greater during full-moon phases. Although much case law supports lighting as an indicator of efforts to provide a safe environment, security specialists are questioning conventional wisdom about lighting. Because so much nighttime lighting goes unused, should it be reduced or turned off? Does an offender look more suspicious under a light or in the dark with a flashlight? Should greater use be made of motion-activated lighting? How would these approaches affect safety and cost-effectiveness? These questions are ripe for research.

ILLUMINATION [3]

Lumens (of light output) per watt (of power input) is a measure of lamp efficiency. Initial lumens per watt data are based on the light output of lamps when new; however, light output declines with use. *Illuminance* is the intensity of light falling on a surface, measured in foot-candles (English units) or lux (metric units). The *foot-candle* (fc) is a measure of how bright the light is when it reaches 1 foot from the source. One lux equals 0.0929 fc. The light provided by direct sunlight on a clear day is about 10,000 fc, an overcast day would yield about 100 fc, and a full moon gives off about 0.01 fc. A sample of outdoor lighting illuminances recommended by the Illuminating Engineering Society of North America are as follows: self-parking area, 1 fc; attendant parking area, 0.20–0.90 fc; covered parking area, 5 fc; active pedestrian entrance, 5 fc; and building surroundings, 1 fc. It generally is recommended that gates and doors, where identification of persons and things takes place, should have at least 2 fc. An office should have a light level of about 50 fc.

Care should be exercised when studying fc. Are they horizontal or vertical? Horizontal illumination may not aid in the visibility of vertical objects such as signs and keyholes. (The preceding fc are horizontal.) The fc vary depending on the distance from the lamp and the angle. If you hold a light meter horizontally, it often gives a different reading that if you hold it vertically. Are the fc initial or maintained?

David G. Aggleton, CPP, stated in a recent article in *Security Technology Executive* (March 2011) that "A quick rule of thumb for minimum reflected light is: (A) Detection: 0.5 fc, (B) Recognition: 1.0 fc, (C) Identification: 2.0 fc are required."

Maintenance and bulb replacement ensure high-quality lighting.

TYPES OF LAMPS [4]

The following lamps are applied outdoors:

- **Incandescent.** These are commonly found at residences. Passing electrical current through a tungsten wire that becomes white-hot produces light. These lamps produce 10–20 lumens per watt, are the least efficient and most expensive to operate, and have a short lifetime of 9,000 hours.
- **Halogen and quartz halogen lamps.** Incandescent bulbs filled with halogen gas (like sealed-beam auto headlights) provide about 25% better efficiency and life than ordinary incandescent bulbs.
- **Fluorescent lamps.** These pass electricity through a gas enclosed in a glass tube to produce light, yielding 40–80 lumens per watt. They create twice the light and less than half the heat of an incandescent bulb of equal wattage and cost 5–10 times as much. Fluorescent lamps do not provide high levels of light output. The lifetime is 9,000–20,000 hours. They are not used extensively outdoors, except for signs. Fluorescent lamps use one-fifth to one-third as much electricity as incandescent with a comparable lumen rating and last up to 20 times longer. They are cost-effective with yearly saving per bulb of $9.00–25.00.
- **Mercury vapor lamps.** They also pass electricity through a gas. The yield is 30–60 lumens per watt and the life is about 20,000 hours.
- **Metal halide lamps.** They are also of the gaseous type. The yield is 80–100 lumens per watt, and the life is about 10,000 hours. They often are used at sports stadiums because they imitate daylight conditions and colors appear natural. Consequently, these lamps complement closed-circuit TV (CCTV) systems, but they are the most expensive lights to install and maintain.
- **High-pressure sodium lamps.** These are gaseous, yield about 100 lumens per watt, have a life of about 20,000 hours, and are energy efficient. These lamps are often applied on streets and parking lots, and through fog are designed to allow the eyes to see more detail at greater distances. They also cause less light pollution then mercury-vapor lamps.
- **Low-pressure sodium lamps.** They are gaseous, produce 150 lumens per watt, have a life of about 15,000 hours, and are even more efficient than high-pressure sodium. These lamps are expensive to maintain.

- **LED (light-emitting diodes).** These are small lights, such as Christmas bulbs, and spotlights. They use very low energy consumption and are long lasting up to 50,000–80,000 hours. This rapidly growing light source may be the light of the future. Currently they are used in many applications such as in garages, street lighting, and rear taillights in motor vehicles.
- **Quartz lamps.** These lamps emit a very bright light and snap on almost as rapidly as incandescent bulbs. They are frequently used at very high wattage—1,500–2,000 watts is not uncommon in protective systems—and they are excellent for use along the perimeter barrier and in troublesome areas.
- **Electroluminescent lights.** These lights are similar to their florescent cousins; however, they do not contain mercury and are more compact.

Each type of lamp has a different *color rendition index* (CRI), which is the way a lamp's output affects human perception of color. Incandescent, fluorescent, and halogen lamps provide an excellent color rendition index of 100%. Based on its high CRI and efficiency the preferred outdoor lamp for CCTV systems is metal halide. Mercury vapor lamps provide good color rendition but are heavy on the blue. Low-pressure sodium lamps, which are used extensively outdoors, provide poor color rendition, making things look yellow. Low-pressure sodium lamps make color unrecognizable and produce a yellow-gray color on objects. People find they produce a strange yellow haze. Claims are made that this lighting conflicts with aesthetic values and affects sleeping habits. In many instances, when people park their vehicles in a parking lot during the day and return to find their vehicle at night, they are often unable to locate it because of poor color rendition from sodium lamps; some even report their vehicles as stolen. Another problem is the inability of witnesses to describe offenders accurately.

Mercury vapor, metal halide, and high-pressure sodium take several minutes to produce full light output. If they are turned off, even more time is required to reach full output because they first have to cool down. This may not be acceptable for certain security applications. Incandescent, halogen, and quartz halogen have the advantage of instant light once the electricity is turned on. Manufacturers can provide information on a host of lamp characteristics including the "strike" and "re-strike" time.

The following sources provide additional information on lighting:

- National Lighting Bureau (http://www.nlb.org): Publications.
- Illuminating Engineering Society of North America (http://www.iesna.org): Technical materials and services; recommended practices and standards; many members are engineers.
- International Association of Lighting Management Companies (http://www.nalmco.org): Seminars, training, and certification programs.

Cost and ROI

Cost is broken down into three categories: (1) 88% energy cost, (2) 8% capital cost, and (3) maintenance cost. ROI is broken down into (1) efficiency and energy savings payback, (2) reduce costs by shutting off unnecessary units, and (3) the concept of going green.

Lighting Equipment

Incandescent or gaseous discharge lamps are used in streetlights. Fresnel lights have a wide flat beam that is directed outward to protect a perimeter and glares in the faces of those approaching. A floodlight "floods" an area with a beam of light, resulting in considerable glare. Floodlights are stationary, although the light beams can be aimed to select positions. The following strategies reinforce good lighting:

1. Locate perimeter lighting to allow illumination of both sides of the barrier.
2. Direct lights down and away from a facility to create glare for an intruder. Make sure the directed lighting does not hinder observation by the patrolling officer.

3. Do not leave dark spaces between lighted areas for burglars to move in. Design lighting to permit overlapping illumination.
4. Protect the lighting system. Locate lighting inside the barrier, install protective covers over lamps, mount lamps on high poles, bury power lines, and protect switch boxes.
5. Photoelectric cells enable light to go on and off automatically in response to natural light. Manual operation is helpful as a backup.
6. Consider motion-activated lighting for external and internal areas.
7. If lighting is required in the vicinity of navigable waters, contact the U.S. Coast Guard.
8. Try not to disturb neighbors by intense lighting.
9. Maintain a supply of portable emergency lights and auxiliary power in the event of a power failure.
10. Good interior lighting also deters burglars. Locating lights over safes, expensive merchandise, and other valuables and having large clear windows (especially in retail establishments) lets passing patrol officers see in.
11. If necessary, join other business owners to petition local government to install improved street lighting.

TWENTY-FIVE THINGS YOU NEED TO KNOW ABOUT LIGHTING [7]

1. **Watts:** Measures the amount of electrical energy used.
2. **Foot-candle:** Measure of light on a surface 1 square foot in area on which one unit of light (lumen) is distributed uniformly.
3. **Lumen:** Unit of light output from a lamp.
4. **Lamp:** Term that refers to light sources that are called *bulbs*.
5. **Lux:** Measurement of illumination.
6. **Illuminare:** Intensity of light that falls on an object.
7. **Brightness:** Intensity of the sensation from light as seen by the eye.
8. **Foot-lambert:** Measure of brightness.
9. **Glare:** Excessive brightness.
10. **Luminaire:** Complete lighting unit; consists of one or more lamps joined with other parts that distribute light, protect the lamp, position or direct it, and connect it to a power source.
11. **Ballast:** Device used with fluorescent and high-intensity discharge lamps to obtain voltage and current to operate the lamps.
12. **High-intensity discharge (HID):** Term used to identify four types of lamps—mercury vapor, metal halide, and high- and low-pressure sodium.
13. **Coefficient of utilization:** Ratio of the light delivered from a luminaire to a surface compared to the total light output from a lamp.
14. **Contrast:** Relationship between the brightness of an object and its immediate background.
15. **Diffuser:** Device on the bottom or sides of a luminaire to redirect or spread light from a source.
16. **Fixture:** A luminaire.
17. **Lens:** Glass or plastic shield that covers the bottom of a luminaire to control the direction and brightness of the light as it comes out of the fixture or luminaire.
18. **Louvers:** Series of baffles arranged in a geometric pattern. They shield a lamp from direct view to avoid glare.
19. **Uniform lighting:** refers to a system of lighting that directs the light specifically on the work or job rather than on the surrounding areas.
20. **Reflector:** Device used to redirect light from a lamp.
21. **Task or work lighting:** Amount of light that falls on an object of work.
22. **Veiling reflection:** Reflection of light from an object that obscures the detail to be observed by reducing the contrast between the object and its background.
23. **Incandescent lamps:** Produce light by passing an electric current through a tungsten filament in a glass bulb. They are the least efficient type of bulb.
24. **Fluorescent lamps:** Second most common source of light. They draw an electric arc

along the length of a tube. The ultraviolet light produced by the arc activates a phosphor coating on the walls of the tube, which causes light.

25. **HID lamps:** Consist of mercury vapor, metal halide, and high- and low-pressure sodium lamps. The low-pressure sodium is the most efficient, but has a very low CRI of 5.

ENERGY MANAGEMENT

The efficiency and management of lighting is becoming a high priority in commissioning new buildings and upgrading existing systems. Indeed, the subject of energy management is expected to become one of the most important considerations within the building regulation documents and have a tremendous impact on the way the construction industry looks at energy. It is apparent that serious measures must now be taken to reduce energy use and waste. This will have an impact on security lighting and the way it is applied. Lighting experts show an increasing urge to work alongside electrical contractors and installers to help them increase their business opportunities by identifying the roles and applications in which energy-efficient lighting should be installed. Electrical contractors are becoming better educated in lighting design that is effective and energy efficient.

Lighting design personnel need to

- Recognize inefficient installations.
- Appreciate the environmental, cost, and associated benefits of energy-efficient lighting schemes.
- Estimate energy cost savings and calculate the payback period.
- Recognize the situations in which expert and specialist knowledge is needed in the design of management systems.
- Think in terms of increasing business while trying to preserve the environment.

At certain points in time, it was said that lighting any system brighter was advantageous. However, we are now seeing a trend away from large floodlights illuminating the night sky with a strong white glare, as exterior lighting is becoming much more focused on the minimum lux levels required. We are also seeing a move toward directional beams.

The lighting industry wants to remove itself from a proliferation of public and private external lighting schemes to counter the light pollution problem and become more energy and cost conscious in its makeup. There must be a mechanism to tackle the problem of countless floodlights, up lighters, spotlights, decorative installations, and an array of security lighting forms that are badly installed and specified, create light pollution, and use high energy levels.

Lighting pollution is now at the forefront of debates for two main reasons:

1. Light pollution spoils the natural effect of the night skies.
2. The greater the light pollution, the greater the power consumption.

Unfortunately, a certain degree of light pollution is needed to satisfy safety and security applications. Equally, there is always the desire to have purely decorative lighting installations, so the answer lies in a compromise. Systems must be designed with a degree of thought given to the avoidance of light pollution and energy waste. External lighting must provide minimal light pollution, a safe environment, and an attractive feature. For attractive features, we can see a greater use of fiber optic solutions with color-changing effects and lighting engineered to direct the illumination downward. Bollards or recessed ground luminaries can be set into walkways so there is no spill into the night sky. Intelligently designed schemes can ensure that lighting is reflected only in a downward direction so that pedestrians are better guided and the lighting has a pleasing effect with little overspill.

Therefore, within the lighting industry, there is a need is to raise standards in all aspects associated with light and lighting, in particular when it comes to energy management and light pollution. We need to define and harness the pleasures

of lighting but at the same time promote the benefits of well-designed energy-efficient schemes among the public at large. There must also be miniaturization and increased lamp life. Energy management must therefore be a part of security lighting.

Lighting Checklist

1. Is all of the perimeter lighted?
2. Is there a strip of light on both sides of fence?
3. Is the illumination sufficient to detect human movement easily at 100 yards?
4. Are lights checked for operation daily prior to darkness?
5. Is extra lighting available at entry points and points of possible intrusion?
6. Are lighting repairs made promptly?
7. Is the power supply for lights easily accessible (for tampering)?
8. Are lighting circuit drawings available to facilitate quick repairs?
9. Are switches and controls
   a. Protected?
   b. Weatherproof and tamper resistant?
   c. Accessible to security personnel?
   d. Inaccessible from outside the perimeter barrier?
   e. Equipped with centrally located master switch(es)?
10. Is the illumination good for guards on all routes inside the perimeter?
11. Are the materials and equipment in receiving, shipping, and storage areas adequately lighted?
12. Are bodies of water on the perimeter adequately lighted?
13. Is an auxiliary source of power available for protective lighting?

Protective Lighting Checklist

1. Is protective lighting adequate on the perimeter?
2. What type of lighting is it?
3. Is the lighting of open areas within the perimeter adequate?
4. Do shadowed areas exist?
5. Are outside storage areas adequately lighted?
6. Are inside areas adequately lighted?
7. Is the guard protected or exposed by the lighting?
8. Are gates and boundaries adequately lighted?
9. Do lights at the gates illuminate the interior of vehicles?
10. Are critical and vulnerable areas well illuminated?
11. Is protective lighting operated manually or automatically?
12. Do cones of light on the perimeter overlap?
13. Are perimeter lights wired in series?
14. Is the lighting at shipping and receiving docks or piers adequate?
15. Is the lighting in the parking lots adequate?
16. Is an auxiliary power source available with backup standby units?
17. Is the interior of buildings adequately lighted?
18. Are top secret and secret activities adequately lighted?
19. Are guards equipped with powerful flashlights?
20. How many more and what types of lights are needed to provide adequate illumination? In what locations?
21. Do security personnel report light outages?
22. How soon are burned-out lights replaced?
23. Are open areas of a campus sufficiently lighted to discourage illegal or criminal acts against pedestrians?
24. Are any areas covered with high-growing shrubs or woods where the light is insufficient?
25. Are the outsides of buildings holding valuable or critical activities or materials lighted?
26. Are interiors of hallways and entrances lighted when buildings are open at night?
27. Are areas surrounding women's dormitories well lighted? Within a college setting?
28. Are campus parking lots lighted sufficiently to discourage tampering with parked cars or other illegal activities?
29. Are areas where materials of high value are stored well lighted? Safes, libraries, bookstores, food storage areas, and so forth?
30. Lamp life versus efficiency?
31. Lamp CRI?

32. Continuous levels of light at night?
33. Provide specific levels of light for CCTV units? We are in the age of HD cameras and HD television monitors as well as low-light cameras, all of which are crime deterrents in some cases.
34. Required light for evening patrols?
35. Complex should have an even and adequate distribution of light?

Lighting Levels

By definition a foot-candle is a unit of illuminance or light falling onto a surface. It stands for the light level on a surface one foot from a standard candle. One foot-candle is equal to one lumen per square foot.

- 0.5 fc for perimeter of outer area
- 0.4 fc for perimeter of restricted area
- 10 fc for vehicular entrances
- 5 fc for pedestrian entrance
- 0.5–2 fc for roadways
- 0.2 fc for open years
- 0.2–5 fc for decks on open piers
- 10–20 fc for interior sensitive structures

Open parking light levels are a minimum of 0.2 fc in low-level activity areas and 2 fc in high-vehicle activity areas. If there is cash collection, the light level is a minimum of 5 fc.

- Loading docks—15 fc
- Loading docks interior—15 fc
- Shipping and receiving—5 fc
- Security gate hous —25–30 fc
- Security gate house interior—30 fc

For pedestrians or normal CCTV cameras the minimum level of light for

- Detection—0.5 fc
- Recognition—1 fc
- Identification—2 fc
- Parking structures—5 fc
- Parking areas or open spaces—2 fc
- Loading docks—0.2–5 fc
- Loading dock parking areas—15–30 fc
- Piers and dock—0.2–5 fc

LIGHTING DEFINITIONS

Lumens

The quantity or flow of light emitted by a lamp is measured in lumens. For example, a typical household bulb rated at 100 watts may output about 1,700 lumens.

Illuminance is the concentration of light over a particular area and is measured in lux, representing the number of lumens per square meter or foot-candles. One foot-candle is equal to 10.76 lux (often approximated to a ratio of 1:10).

Note: When evaluating the amount of light needed by a particular CCTV camera (or the eye) to perceive a scene, it is the amount of light shining over the area of the lens iris (camera or eye), or its luminance, that is critical.

Reflectance

When we see an object our eyes are sensing the light reflected from that object. If there is no light reflected from the object, we only see a silhouette in contrast to its background. If the object is illuminated by other than white light we will see the object in colors that are not true. The color of the surface also impacts reflectance; a light surface, such as a parking lot paved in concrete, will have higher reflectance than a dark surface (a parking lot paved in asphalt or black-top). The measure of reflectance of an object is the ratio of the quantity of light (measured in lumens) falling on it to the light reflected from it, expressed as a percentage.

CRI

The ability of a lamp to faithfully reproduce the colors seen in an object is measured by the CRI. Security personnel need the ability to accurately describe color. It is an important aspect in the apprehension of criminals who are caught on CCTV displays and recordings. CRI is measured on a scale of 1 to 100. A CRI of 70–80 is considered good, above 80 is considered excellent, and 100% is considered daylight.

Corrected Color Temperature

A measure of the warmth or coolness of a light is the corrected color temperature (CCT). It has a considerable impact on mood and ambiance of the surroundings.

Lighting Systems

A lighting system consists of a number of components, all of which are important to the effectiveness of a lighting application. Following is a list of the major components and their functions:

- **Lamp (also known as a lightbulb).** Manufactured light source that includes the filament or an arc tube, its glass casing, and its electrical connectors. Types of lamps include incandescent and mercury vapor, which describe the types of technologies used to create the light.
- **Luminary (also known as fixture).** Complete lighting unit consisting of the lamp, its holder, and the reflectors and diffusers used to distribute and focus the light.
- **Mounting hardware.** Examples are a wall bracket or a light pole used to fix the correct height and location of the luminary.
- **Electrical power.** Operates the lamp, ballasts, and photocells. Some lamp technologies are sensitive to reduced voltage, in particular the HID family of lamps (metal halide, mercury vapor, and high-pressure sodium).

REFERENCES

[1] Purpura P. Police activity and the full moon. J Police Science Administration 1979;7(3):350.
[2] Berube H. New notions of night light. Secur Manage 1994:29–33.
[3] National Lighting Bureau. Lighting for safety and security. Washington, DC: National Lighting Bureau; n.d., p. 1–36; Smith, MS. Crime prevention through environmental design in parking facilities. Washington, DC: National Institute of Justice, 1996, p. 1–4; Bowers, DM. Let there be light. Security Management 1995, p. 103–111; Kunze, DR, Schiefer, J. An illuminating look at light. Security Management 1995, p. 113–116.
[4] Fischer RJ, Halibozek E, Green G. Introduction to security. 8th ed Boston: Butterworth-Heinemann; 2008.
[5] Tyska LA, Fennelly LJ. Physical security: 150 things you should know. Boston: Butterworth-Heinemann; 2000.

WEB SITES

National Lighting Bureau: www.nlb.org.
Illuminating Engineering Society: www.iesna.org.
International Association of Light Management Companies: www.nalmco.org.

APPENDIX 9.A. LIGHTING DESCRIPTION

TABLE 9-1 Lighting Types

Type	CRI	Light Color
Incandescent	100	White Reflects all light
Fluorescent	62	Bluish/white Good color rendition
Mercury vapor	15	Blue/green Fair color rendition When used as a streetlight, there will be a blue label indicating wattage
High-pressure sodium	22	Golden/white Poor color rendition When used as a streetlight, there will be a yellow label indicating wattage
Low-pressure sodium	44	Yellow Very low color rendition
Metal halide	65–90	Bright white Very high color rendition When used as a streetlight, there will be a white label indicating wattage
Halogen/quartz halogen	100	White
LED	95–98	White
Induction	80–100	White

TABLE 9-2 Operation Costs (10 years)

Technology	Wattage	Lamp Changes	Energy	Maintenance	Material	Operation Cost
High-pressure sodium	70	3.7	$927	$201	$73	$1,201
High-pressure sodium	150	3.7	$1,971	$201	$73	$2,245
High-pressure sodium	250	3.7	$3,154	$201	$73	$3,427
High-pressure sodium	400	3.7	$4,878	$201	$73	$5,151
High-pressure sodium	1,000	3.7	$11,563	$201	$224	$11,988
Induction	40	0	$429	$0	$0	$429
Induction	80	0	$858	$0	$0	$858
Induction	100	0	$1,072	$0	$0	$1,072
Induction	120	0	$1,287	$0	$0	$1,287
Induction	200	0	$2,144	$0	$0	$2,144
Metal halide (V)	150	5.8	$1,971	$321	$187	$2,479
Metal halide (V)	175	8.8	$2,263	$482	$278	$3,022
Metal halide (V)	250	8.8	$3,101	$482	$280	$3,863
Metal halide (V)	400	8.8	$4,793	$482	$280	$5,556
Metal halide (V)	1,000	7.3	$11,248	$402	$365	$12,014
Metal halide (H)	150	7.8	$1,971	$428	$249	$2,648
Metal halide (H)	175	11.7	$2,263	$642	$370	$3,275
Metal halide (H)	250	11.7	$3,101	$642	$374	$4,117
Metal halide (H)	400	11.7	$4,793	$642	$374	$5,810
Metal halide (H)	1,000	9.7	$11,248	$535	$487	$12,270
Low-pressure sodium	180	5.5	$2,308	$301	$345	$2,954
Low-pressure sodium	135	5.5	$1,873	$301	$257	$2,432
Low-pressure sodium	90	5.5	$1,306	$301	$203	$1,809
Low-pressure sodium	55	4.9	$838	$268	$161	$1,267
Low-pressure sodium	35	4.9	$629	$268	$161	$1,057

Based on 24 hours of on time, 0.12 kW/hour, and $55/hour labor charge.
Source: U.S. Energy Technologies, 2007.
Formula to determine the cost to operate a light source:
Watts × Hours = Watts Hours
Watts × Hours ÷ 1,000 = Kilowatts
Kilowatts × Rate = Cost
Information for the formula:
Watts: On the bulb or fixture of the light source
Watt × Hours ÷ 1,000 = Kilowatts
Kilowatts × Rate = Cost
Source: U.S. Department of Energy, 2009.

CHAPTER

10

Alarms: Intrusion Detection Systems*

Stephen McKinnon, CPP

Burglary is a big business. Moreover, crime figures show a staggering rate of increase for burglaries of private homes. It is no wonder then that many homeowners and business owners are giving serious consideration to electronic alarm protection. Alarm operators are in the market to make a fast dollar, and the unwary customer who buys what seems to be a bargain too often ends up being cheated.

The selection of a proper alarm system is not a simple matter, because the needs of each homeowner or business owner are different, like a set of fingerprints. Some factors that determine the requirements of an individual alarm system and the questions that must be answered when selecting a system include:

1. The threat or risk. What is the system to protect against?
2. The types of sensors needed. What will be protected?
3. What methods are available to provide the level of protection needed?
4. The method of alarm signal transmission. How is the signal to be sent and who will respond?

Most of the confusion regarding intrusion detection systems is a result of the variety of methods available to provide the protection needed. The combinations of detection methods are in the thousands. An intrusion detection system may deter a would-be intruder. However, the primary function of the alarm system is to signal the presence of an intruder. An intrusion detection system can be just a portion of the overall protection needed. Many large businesses supplement these systems with security guards and other security personnel. The successful operation of any type of an alarm system depends on its proper installation and maintenance by the alarm installing company and the proper use of the system by the customer.

COMPONENTS OF ALARM SYSTEMS

Sensing devices are used in the actual detection of an intruder (Figures 10-1 and 10-2). Each has a specific purpose and can be divided into three categories: perimeter protection, area/space protection, and object/spot protection.

Perimeter Protection

Perimeter protection is the first line in the defense to detect an intruder. The most common points

* This material was originally complied by Lawrence J. Fennelly, Mike Rolf, and James Culley.

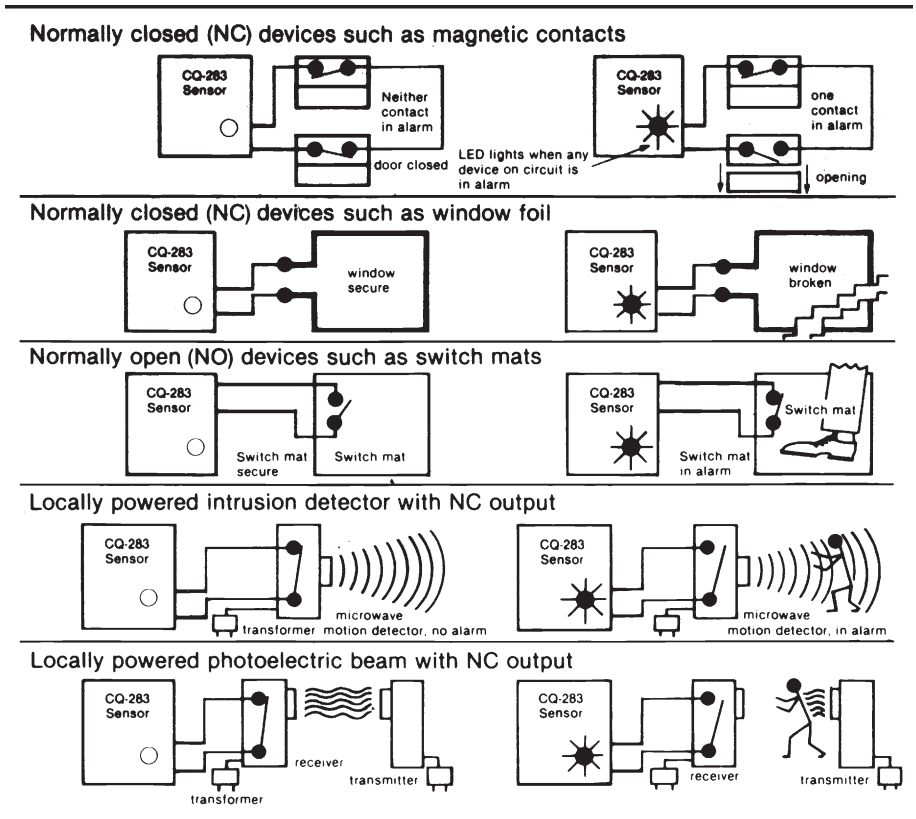


FIGURE 10-1 Typical application of the use of magnetic contacts, window foil, switch mats, motion detection, and photoelectric beam. *(Courtesy of Aritech Corporation.)*

equipped with sensing devices for premise perimeter protection are doors, windows, vents, skylights, or any opening to a business or home. Since over 80% of all break-ins occur through these openings, most alarm systems provide this type of protection. The major advantage of perimeter protection is its simple design. The major disadvantage is that it protects only the openings. If the burglar bursts through a wall, comes through the ventilation system, or stays behind after closing, perimeter protection is useless.

1. **Door switches.** These are installed on a door or window in such a way that opening the door or window causes a magnet to move away a contact switch, which activates the alarm. They can be surface mounted or recessed into the door and frame. A variety of types of switches are manufactured for all types of doors and windows. The switches are both wide gap type and magnetic standard type.
2. **Glass break detectors.** These detectors are attached to the glass and sense the breakage of the glass by shock or sound. Glass breakage sensors use microphone transducers to detect the glass breakage. A ceiling sensor over a window covers a 30° radius.
3. **Wooden screens.** These devices are made of wooden dowel sticks assembled in a cage-like fashion no more than 4 inches from each other. A very fine, brittle wire runs in the wooden dowels and frame. The burglar must break the doweling to gain entry and thus break the low-voltage electrical circuit, causing the alarm. These devices are used primarily in commercial applications.

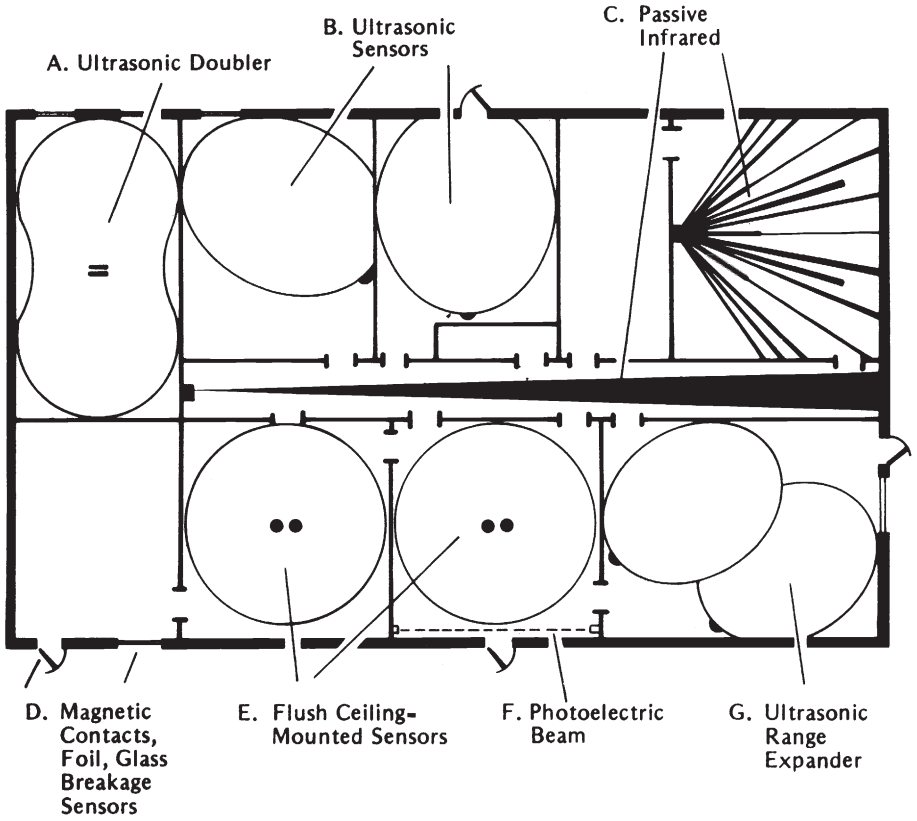


FIGURE 10-2 Sensors. (A) Ultrasonic doubler: back-to-back ultrasonic transceivers provide virtually double the coverage of single detectors at almost the same wiring and equipment cost. With more than 50 × 25 feet of coverage, the doubler is the best value in space protection. (B) Ultrasonic sensors: easy to install, no brackets needed. Can be mounted horizontally, vertically, or in a corner; surface, flush, or with mounting feet on a shelf. Each UL-listed sensor protects a three-dimensional volume up to 30 feet wide and high. (C) Passive infrared: for those zones where the lower-cost ultrasonic sensor is inappropriate, there is no need to buy a complete passive infrared system as both ultrasonic and passive infrared can be used in the same system. (D) Magnetic contacts, foil, glass breakage sensors: the building's perimeter protection detectors can be wired into the system via universal interface sensor. There is no need for running a separate perimeter loop. (E) Flush ceiling-mounted sensors: only the two small 2-inch diameter transducer caps are visible below the ceiling tiles. Designed for where minimum visibility is needed for aesthetic or security purposes. (F) Photoelectric beam: the universal interface sensor allows the connection of any NO or NC alarm device into the system for zoned annunciation. It can be used with photoelectric beams, switch matting, microwave motion detectors, and many other intrusion detectors. (G) Ultrasonic range expander: adding an ultrasonic range expander can increase the coverage of an ultrasonic sensor by 50–90%, depending on where it is positioned and the surrounding environment. *(Courtesy of Aritech Corporation.)*

4. **Window screens.** These devices are similar to regular wire window screens in a home except that a fine, coated wire is a part of the screen. When the burglar cuts the screen to gain entry, the flow of low-voltage electricity is interrupted and causes the alarm. These devices are used primarily in residential applications.
5. **Lace and panels.** The surfaces of door panels and safes are protected against entry by installing a close lace-like pattern of metallic foil or a fine brittle wire on the surface. Entry cannot be made without first breaking the foil or wire, thus activating the alarm. A panel of wood is placed over the lacing to protect it.

6. **Interior sensors.** They come in many shapes and sizes depending upon the application, for example, interior motion detector units and proximity and boundary penetration.

Area/Space Protection

Area/space protection devices (Table 10-1) protect the interior spaces in a business or home. They protect against intrusion whether or not the perimeter protection was violated. It is particularly effective against a stay-behind intruder or the burglar who cuts through the roof or breaks through a block wall.

Space protection devices are only a part of the complete alarm system. They should always be supplemented with perimeter protection. The major advantage of space protection devices is that they provide a highly sensitive, invisible means of detection. The major disadvantage is that improper application and installation by the alarm company can result in frequent false alarms.

The types of area/space protection include:

1. **Photoelectric eyes (beams).** These devices transmit a beam across a protected area. When an intruder interrupts the beam, the beam circuit is disrupted and the alarm initiated. Photoelectric devices use a pulsed infrared beam that is invisible to the naked eye. Some units have a range of over 1,000 feet and can be used outdoors, although they are rarely used today.
2. **Ultrasonics.** They (although rarely used today) work on a low-frequency sound wave projected from the unit. The frequency is in kilohertz (23–26) and its area of coverage can be anywhere from 5 to 40 feet in length. The pattern is volumetric and cannot be aimed, although the pattern may be directed by the use of deflectors. Deflectors come in 90° or 45° angles. A doubler type uses two 45° angles back to back. Ultrasonics work on a change in frequency, called the *Doppler effect*. A motion detector has two transducers; the transmitter sends out a signal that is bounced back to the receiver by immobile objects in the protected area. If an intruder moves toward or away from the unit, the change in its reflected frequency signals an alarm. Ultrasonics may be found as stand-alone units or part of what is called a *master system*. The stand-alone units compare the reflected signal within the unit and trip the control panel by opening or closing a relay contact. Master systems work by sending the signal back to a main processing unit. The main processing unit compares the signal and trips the relay contacts of the processor. False alarms result from three types of sources:
   - **Motion.** Objects that move in the path of protection and air turbulence are seen as motion because of the frequency of the unit.
   - **Noise.** Ultrasonic noise is present when audible noises are heard; hissing (such as from high-pressure air leaking or steam radiators) or bells ringing can be a source of these noises.
   - **Radio or electrical interference.** Induced electrical signals or radio frequency (RF) interference from radio transmitters can cause false alarms.
3. Grounding and shielding are both very important in a master system. If an earth ground is required, it should be a cold water pipe. The length of the ground wire should be as short as possible and with a minimum number of bends. Potential problems include:
   - Turbulence and draft, hanging displays, moving draperies, and small pets.
   - Noise caused by air hissing, bells, and telephones.
   - Temperature or humidity can affect range of the ultrasonic unit.
4. Carpets, furniture, and draperies may absorb some of the signal, decreasing the unit's sensitivity. Ultrasonic energy does not penetrate most objects. The signal may be reflected off some smooth surfaces.
5. **Microwave.** Microwave detectors are a volumetric type of space protection and are based

TABLE 10-1 Motion Sensor Survey Checklist

Environmental and Other Factors Affecting Sensor Usage	Effect on Sensor				
Circle One	Ultrasonics	Microwave	Passive IR	Recommendation and Notes	
If the areas to be protected are enclosed by thin walls or contain windows, will there be movement close to the outside of this area?	Yes No	None	Major	None	Avoid using a microwave sensor unless it can be aimed away from thin walls, glass, etc., which can pass an amount of microwave energy.
Will the protection pattern see sun, moving headlamps, or other sources of infrared energy passing through windows?	Yes No	None	None	Major	Avoid using a PIR sensor unless the pattern can be positioned to avoid rapidly changing levels of infrared energy.
Does the area to be protected contain HVAC ducts?	Yes No	None	Moderate	None	Ducts can channel microwave energy to other areas; if using a microwave sensor, aim it away from duct openings.
Will two or more sensors of the same type be used to protect a common area?	Yes No	None	None (see Note)	None	Note: Adjacent units must operate on different frequencies.
Does the area to be protected contain fluorescent or neon lights that are on during the protection-on period?	Yes No	None	Major	None	Microwave sensor, if used, must be aimed away from any fluorescent or neon light within 20 feet.
Are incandescent lamps cycled on and off during the protection-on period included in the protection pattern?	Yes No	None	None	Major	If considering use of a PIR sensor, make a trial installation and, if necessary, redirect the protection pattern away from incandescent lamps.
Must the protection pattern be projected from a ceiling?	Yes No	None, but only for ceiling heights up to 15 feet	Major	Major	Only ultrasonic sensors can be used on a ceiling, but height is limited to 15 feet; at greater ceiling heights, use rigid ceiling brackets to suspend the sensor to maintain the 15-foot limitation or, in large open areas, try a microwave sensor mounted high on a wall and aimed downward.

Continued

TABLE 10-1 Motion Sensor Survey Checklist—cont'd

Environmental and Other Factors Affecting Sensor Usage	Effect on Sensor				
Is the overall structure of flimsy construction (corrugated metal, thin plywood, etc.)?	Yes No	Minor	Major	Minor	Do not use a microwave sensor; where considerable structural movement can be expected, use a rigid mounting surface for an ultrasonic or PIR sensor.
Will the protection pattern include large metal objects or wall surfaces?	Yes No	Minor	Major	Minor (major if metal is highly polished)	Use an ultrasonic sensor or use a PIR sensor.
Are any radar installations nearby?	Yes No	Minor	Major when radar is close and sensor is aimed at it	Minor	Avoid using a microwave sensor.
Will the protection pattern include heaters, radiators, air conditioners, or the like?	Yes No	Moderate	None	Major when rapid changes in air temperature are involved	Use an ultrasonic sensor, but aim it away from sources of air turbulence (desirable to have heaters, etc., turned off during protection-on period), or use a microwave sensor.
Will the area to be protected be subjected to ultrasonic noise (bells, hissing sounds)?	Yes No	Moderate, can cause problems in severe cases	None	None	Try muffling the noise source and use an ultrasonic sensor, use a microwave sensor, or use a PIR sensor.
Will the protection pattern include drapes, carpet, racks of clothing, or the like?	Yes No	Moderate, reduction in range	None	Minor	Use an ultrasonic sensor if some reduction in range can be tolerated or use a microwave sensor.
Is the area to be protected subject to changes in temperature and humidity?	Yes No	Moderate	None	Major	Use an ultrasonic sensor unless changes in temperature and humidity are severe or use a microwave sensor.
Is there water noise from faulty valves in the area to be protected?	Yes No	Moderate, can be a problem	None	None	If noise is substantial, try correcting faulty valves and use an ultrasonic sensor, use a microwave sensor, or use a PIR sensor.

Environmental and Other Factors Affecting Sensor Usage	Effect on Sensor				
Will the protection pattern see moving machinery, fan blades, or the like?	Yes No	Major	Major	Minor	Have machinery, fans, and the like turned off during the protection-on period, carefully place an ultrasonic sensor, or use a PIR sensor.
Will drafts or other air movement pass through the protection pattern?	Yes No	Major	None	None, unless rapid temperature changes are involved	If the protection pattern can be aimed away from air movement or air movement can be stopped during the protection-on period, use an ultrasonic sensor, use a microwave sensor, or use a PIR sensor.
Will the protection pattern see overhead doors that can be rattled by wind?	Yes No	Major	Major	Minor	If the protection pattern can be aimed away from such doors, use an ultrasonic sensor or use a PIR sensor.
Are there hanging signs, calendar pages, or the like that can be moved by air currents during the protection-on period?	Yes No	Major	Major	Moderate, can be a problem	Use an ultrasonic sensor, but aim the pattern away from objects that can move or remove such objects, or use a PIR sensor.
Are adjacent railroad tracks used during the protection-on period?	Yes No	Major	Minor	Minor	A trial installation is required if using an ultrasonic sensor.
Can small animals (or birds) enter the protection pattern?	Yes No	Major	Major	Major (particularly rodents)	Install a physical barrier to prevent intrusion by animals or birds.
Does the area to be protected contain a corrosive atmosphere?	Yes No	Major	Major	Major	None of these sensors can be used.

on a Doppler shift. They detect intruders by the use of a radiated RF electromagnetic field. The unit operates by sensing a disturbance in the generated RF field, called the Doppler effect. The frequency range is between 0.3 and 300 GHz (1 GHz = 1 billion cps). Any type of motion in the protected area creates a change in frequency, causing an alarm condition. Because the power output from the unit is relatively low, the field radiated is harmless. Microwave energy penetrates most objects and reflects off of metal. One of the most important considerations in placement of these units is vibration. The microwave must be mounted on a firm surface: Cinder block, brick, or main support beams are ideal mounting locations. Never mount two microwave units with identical frequencies in the same room or area where the patterns may overlap. This could cause cross talk between the units, causing false alarms. Microwave units draw excessive current, so the proper gauge of wire should be used and the length of the wire run should also be taken into consideration. Current readings should be taken at the end of an installation or while troubleshooting units to ensure that the maximum current of the control panel has not been exceeded. Fluorescent lights may be a problem because the radiated ionization from the lights may be seen as motion by the detector. Potential problems include:

- Vibrations or movement of mounting surfaces, or mounts on a wall, sense change in electrical current.
- Reflection of pattern or movement of metal objects in a protected area, such as moving fan blades of movement of overhead doors.
- Penetration of thin walls or glass is a potential problem if motion or large metal objects, such as trains or cars, are present.
- Radio frequency interference (RFI), radar, or AC line transients in severe cases can be a problem.
- Water movement in plastic or PVC storm drains is a potential interference if located close to the unit. Most microwave units provide a test point, where the amplifier output voltage can be read. By following the manufacturer's recommended voltage settings the microwave can be set up properly and the unit environment examined.

6. **Passive infrared motion detectors.** These detectors are passive sensors, because they do not transmit a signal for an intruder to disturb. Rather, a source of moving infrared radiation (the intruder) is detected against the normal radiation/temperature environment of the room. Passive infrared detectors (PIRs) detect a change in the thermal energy pattern caused by a moving intruder in the field of view of the detector. The field of view of an infrared unit must terminate on an object to ensure its proper operation and stability. An infrared unit should never be set up to look out into midair. Potential problems include:
   - Turbulence and drafts are a problem if the air is blowing directly on the unit or causes a rapid change in temperature of objects in the path of protection.
   - Stray motion (i.e., drapes blowing, hanging objects or displays, small animals).
   - Changing temperatures (i.e., hotspots in machinery, sunlight) may cause false alarms. The temperature of the background infrared level may also affect the unit's sensitivity: PIRs become less sensitive as the temperature increases.
   - Lightning or bright lights, such as halogen headlights. The infrared radiation pattern is blocked by solid objects as it is unable to penetrate most objects. The pattern of protection may also be affected by reflection off smooth surfaces.
7. **Pressure mats.** These mats are basically mechanical switches. Pressure mats are most frequently used as a backup system to perimeter protection. When used as traps they can be hidden under the carpet in front of a likely target or in hallways where an intruder would travel.
8. **Sound sensors.** These sensors detect intrusion by picking up the noise created by a

burglar during an attempt to break into a protected area. These sensors consist of a microphone and an electronic amplifier/processor. When the sound level increases beyond the limit normally encountered, the unit signals an alarm. Some units have pulse-counting and time-interval features. Other types can actually listen to the protected premises from a central monitoring station.

9. **Dual-technology sensors.** Dual-technology sensors, commonly referred to as *dual-techs*, are a combination of two types of space-protection devices. The principle of the unit is that both sections of the detectors must be tripped at the same time to cause an alarm. A dual-tech unit could be a combination passive/microwave or a combination passive/ultrasonic. By using a dual-technology device, an installer can provide space protection in areas that may have presented potential false alarm problems when a single-technology unit was used. Repair people can replace units sending false signals because of environment or placement. Dual-techs are not the solution to all false alarm problems, and unless careful consideration is used in installing or replacing a device, the false alarm problems may persist. Since these contain two different types of devices, there is much more to consider. Dual-techs draw much more current than conventional detectors. Current readings are essential and additional power supplies may be necessary to provide enough operating current and standby power. Until recently, if one section of the unit stopped working or was blocked off in some way by the end user, the unit was rendered inoperable. Manufacturers are only now working on supervising the microwave section of these units. If the unit is located or adjusted so that one section of the unit is continuously in an alarm condition, the dual-technology principle is worthless.
10. **Interior sensors.** Are generally active or passive, covert or visible, or volumetric or line applications.

False Alarms

There are three hard-core reasons for false alarms, and the secret to reducing them is to clearly identify the cause and make proactive corrections.

1. Lack of proper education on how to enter and exit the complex, such as improper arming and disarming of the keypad
2. Weather
3. Equipment failure (dead batteries) and installation problems

APPLICATION

For all practical purposes, the reason we use space protection is as a backup to the perimeter system. It is not necessary to cover every inch of the premises being protected. The best placement is as a trap in a high-traffic area or spot protection for high-value areas. The worst thing an installer can do is overextend the area being protected by an individual unit (e.g., trying to cover more than one room with a detector or trying to compensate for placement or environment by overadjusting the sensitivity). By using a little common sense and checking for all possible hazards, you can ensure a trouble-free installation. Make sure that the units have adequate power going to each head and the standby batteries are working and charging properly. Be sure to adjust for pets and brief customers and any problems they may create, such as leaving fans or machinery on, and not to open windows in the path of protection. Before leaving an installation, make sure that all units have been walk-tested and the areas in question have been masked out. One of the most important considerations in setting up a number of space protection devices is *zoning*. Never put more than two interior devices in one zone if at all possible. The majority of false alarms are caused by interior devices. Breaking up the interior protective circuits as much as possible gives the service person a better chance of solving a false alarm problem (even with two heads in one zone you have a 50/50 chance of finding the trouble unit). Zoning a system correctly helps

with troubleshooting, makes the police department feel better about the company and the company feel better about the installer, and ensures good relations with the customer.

Object/Spot Detection

Object/spot detection is used to detect the activity or presence of an intruder at a single location. It provides direct security for objects. Such a detection method is the final stage of an in-depth system for protection. The objects most frequently protected include safes, filing cabinets, desks, art objects, models, statues, and expensive equipment. The types of object/spot protection are:

1. **Capacitance/proximity detectors.** The object being protected becomes an antenna, electronically linked to the alarm control. When an intruder approaches or touches the object/antenna, an electrostatic field is unbalanced and the alarm is initiated. Only metal objects can be protected in this manner.
2. **Vibration detectors.** These devices utilize a highly sensitive, specialized microphone called an *electronic vibration detector* (EVD). The EVD is attached directly to the object to be protected. It can be adjusted to detect a sledgehammer attack on a concrete wall or a delicate penetration of a glass surface. It sends an alarm only when the object is moved, whereas capacitance devices detect when the intruder is close to the protected object. Other types of vibration detectors are similar to tilt switches used in pinball machines.

Alarm Control

All sensing devices are wired into the alarm control panel that receives their signals and processes them. Some of the most severe burglary losses are caused not by a failure in equipment but simply by someone turning off the alarm system. The type of control panel needed depends on the sophistication of the overall intrusion alarm system. Some control panels provide zoning capabilities for separate annunciation of the sensing devices. Others provide the low-voltage electrical power for the sensing devices.

Included in the control panel is the backup or standby power in the event of an electrical power failure. Batteries are used for standby power. Some equipment uses rechargeable batteries; the control has a low-power charging unit (a trickle charger) and maintains the batteries in a fully charged condition.

Modern control panels use one or more microprocessors. This allows the control panel to send and receive digital information to the alarm station. An alphanumeric pad can display zone information as well as supervisory conditions. Each user can also have a unique code, allowing restriction during specified times or limiting access into certain areas. By using individual code numbers, the alarm control panel can track activity as well as transmit this information off-site.

If the alarm control panel is connected to a central monitoring station, the times that the system is turned on and off are recorded and logged. When the owner enters the building in the morning, a signal is sent. If this happens at a time prearranged with the central station, it is considered a normal opening. If it happens at any other time, the police are dispatched.

The owner or other authorized persons can enter the building during the closed times. The person entering must first call the central station company and identify himself or herself by a special coding procedure. Records are kept at the central station company for these irregular openings and closings.

Tamper protection is a feature that generates an alarm signal when the system is compromised in any way. Tamper protection can be designed into any or all portions of the alarm system (control panel, sensing devices, loop wiring, alarm transmission facilities).

Alarm Transmission/Signaling

The type of alarm transmission/signaling system used in a particular application depends on the location of the business or residence, the frequency of police patrols, and the ability of the

customer to afford the cost. Remember, after deterrence, the purpose of an alarm is to summon the proper authorities to stop a crime during its commission or lead to the apprehension of the intruder. It is very important that the response by proper authorities to the alarm comes in the shortest possible time. Two types of alarm signaling systems are in general use:

1. **Local alarm.** A bell or light indicates that an attempted or successful intrusion has taken place. The success of the system relies on someone hearing or seeing the signal and calling the responsible authorities. The local alarm also notifies burglars that they have been detected. This may be advantageous in frightening off the less-experienced intruder.
2. **Central station system.** The alarm signal is transmitted over telephone lines to a specially constructed building called the central station. Here, trained operators are on duty 24 hours a day to supervise, record, and maintain alarms. On receipt of an alarm, the police are dispatched and, in some cases, the alarm company guard or runner. The record-keeping function and guard response ensure thorough documentation of any alarm signal. There are seven types of alarm transmissions to the central station. Each type of transmission has certain advantages and disadvantages that must be considered in determining the risk. Transmission of an alarm signal to the Underwriters Laboratories (UL)-listed central station is generally regarded as the most reliable method for reducing the burglary losses.
    1. **Direct wire systems.** High-risk locations (banks, jewelers, furriers) are generally protected with a direct wire system. A single dedicated telephone line is run from the protected premises to the central station or police station, where a separate receiver supervises only that alarm. A fixed DC current is sent from the central station to the protected premises and read on a meter at the central station. The advantage of a direct wire system is that problems can be traced very quickly to a specific alarm system. This makes compromising the alarm signal by a professional burglar more difficult. The disadvantage of such a system is the higher cost of leased telephone lines. This becomes a more serious economic factor as the distance from the central station to the protected premises increases. Proper transmission of the alarm signal to the central station is essential. Problems can result on these telephone lines from shorts and broken wires. Most central stations expect these problems and are well equipped to rapidly make repairs. However, some of today's burglars are more sophisticated. They know they can prevent the transmission of the alarm signal to the central system by shunting or jumpering out the leased telephone line. Special methods are used by the alarm company to protect against jumpering of the alarm signal. Alarm systems having this special line security are classified as AA Grade Central Station alarms by UL.
    2. **Circuit (party line) systems.** Alarm signals transmitted over circuit transmission systems can be compared to a party line where several alarm customers defray the cost of the telephone line by sharing it. With a circuit transmission system, as many as 15 alarm transmitters may send alarm signals to a single receiving panel at the central station over the same line or loop. The alarm signals at the central station are received on strips of paper. Each alarm has a distinct code to identify it from others. The advantage of a circuit-loop alarm transmission system is the lower telephone line cost. Thus, a central station can make its services available to more customers by subdividing the cost of the telephone line among different users. The disadvantage of circuit-loop alarm transmission systems is that problems on a leased telephone line are more difficult to locate than with a direct wire system.

3. **Multiplex systems.** The multiplex system is designed to reduce leased telephone line charges while providing a higher degree of line security than circuit-loop alarms. Multiplex systems introduced data processing (computer-based techniques) to the alarm industry.
4. **Digital communicators.** This computer-based type of alarm transmission equipment sends its signal through the regular switch line telephone network. The alarm signal transmitted is a series of coded electronic pulses that can be received only on a computer terminal at the central station.
5. **Telephone dialer.** The dialer delivers a prerecorded verbal message to a central station, answering service, or police department when an alarm is activated. Many of the earlier tape dialers were a source of constant problems to police departments, because of their lack of sophistication. Basically, they were relabeled tape recorders. It was not uncommon for the tape dialer to play most of the message before the police could answer the phone. The police knew that an alarm signal had been sent, but did not know its location. The newer, modern tape dialers have solved these problems.
6. **Radio signal transmission.** This method takes the alarm signal from the protected premises and sends it via radio or cellular phone to either a central station or police dispatch center. Additionally, the alarm signal can be received in a police patrol car.
7. **Video verification.** Along with standard alarm transmissions, video images are sent to the central station. This provides for a higher level of protection while helping to eliminate false alarms by allowing central station operators to see what is happening inside the protected area. With the increase of the false police dispatches, video verification is playing a major role in the battle against false alarms.

Alarms Deter Crime

False alarms waste police resources and alarm company resources. The police and alarm industry are acutely aware of this, and both have initiated efforts across the country to relieve the dilemma.

The National Crime Prevention Institute has long endorsed alarm systems as the best available crime deterrent. This education institution realizes that most criminals fear alarm systems; they much prefer to break into an unprotected building rather than risk capture by a hidden sensor.

Problem deterrence is the alarm business, a field that, in fact, extends far beyond protecting premises from burglary. The crisis prevention duties of alarm firms range from monitoring sprinkler systems and fire sensors and watching temperature levels in buildings to supervising industrial processes such as nuclear fission and the manufacturing of dangerous chemicals.

To alarm companies, deterrence is a sophisticated, specialized art. In the area of crime prevention, companies take pride in spotting potential weaknesses in a building and designing an alarm system that confounds the most intelligent criminals.

Crime prevention is the area where police need the most help. The rise in burglary and other crimes has often put police officers in a response posture.

False Alarms

The full crime prevention potential in alarm systems has yet to be realized. Relatively speaking, the number of premises not protected by alarms is great, although those businesses and residences holding the most valuable goods are thoroughly guarded by the most sophisticated sensor systems.

Yet the main drag on the potential of alarms, as industry leaders and police are aware, remains the false alarm problem. A modern instance of the boy who cried "wolf," false alarms erode the effectiveness of alarm systems. They are costly to alarm companies and police agencies.

It is a fact that alarm systems prevent crime. These electronic and electrical systems deter burglars, arsonists, vandals, and other criminals. They are both the most effective and most economical crime prevention tool available.

Police budgets have been reduced in most locales and frozen in others, while private investment in alarm security is growing yearly.

The National Burglary and Fire Alarm Association (NBFAA) asked its members to rank their priorities on association activities. The outstanding response asked for a comprehensive program to help member companies reduce false alarms. Moreover, while researching possible programs, the NBFAA learned that many members had already embarked on significant reduction efforts.

Some police departments initiated a written letter program from the police chief to those who have an excessive number of alarm runs. Others have the crime prevention officer make a follow-up visit to the business or residence. After the other steps have failed, many police departments are assessing false alarm fines.

By protecting such places as hospitals, office buildings, and schools, alarm systems free up police resources and enable patrol officers to spend more time in areas with high crime rates and fewer premises protected by alarm systems. Police may also dedicate more officers to apprehending criminals. In this manner, police and alarm companies work together, complementing one another and waging a mutual war on crime.

ALARM EQUIPMENT OVERHAUL

A California alarm station undertook a major overhaul. The effort began with a false alarm inventory, in which subscribers whose systems produced four or more false alarms per week were weeded out. Service workers then replaced—virtually reinstalled—the alarm systems for those subscribers. New sensors, new batteries, new wiring, and new soldering jobs were required in many instances. The process was costly, but it paid off in the long run. The office then had fewer service calls and an improved relationship with the local police that increased business.

Many NBFAA member companies instituted training programs for their sales, installation, and service personnel. Also, subscribers are educated on the operation of their systems three times: by salespeople, by installers, and by supervisors when they inspect newly installed systems.

One member company weeded out and entirely rebuilt its problem systems. This approach is the most feasible way for smaller firms to attack the problem. Lacking sufficient capital to initiate a comprehensive program, such companies can, nevertheless, cut down the number of false alarms by renovating the relatively few systems that cause the majority of problems.

Police chiefs and crime prevention officers working in areas troubled by false alarms should meet with the heads of the firms in their areas and discuss reduction programs like these.

ADDITIONAL RESOURCES

NBFAA members have a guide in the form of a comprehensive quality control manual outlining measures they can undertake to alleviate false alarms. To provide an idea of what is inside the *False Alarm Handbook*, an outline of it follows:

1. Determine false alarm rate and causes.
2. Form an alarm equipment evaluation committee.
3. Institute equipment testing procedures.
4. Develop equipment training facilities.
5. Know how to plan and make alarm installations.
6. Be familiar with sensor zoning procedures.
7. Inspect installations.
8. Educate the subscriber.
9. Cooperate with local law enforcement officers.

The theory behind the handbook is evident in the section titles. Companies are encouraged to begin with a series of statistical studies, from the general false alarm rate per total alarms and systems to causes distinguishing among equipment, user, telephone line, and environmental problems. A separate study helps companies determine how much money false alarms cost them.

The results of these studies should then be reviewed by the company's alarm equipment evaluation committee. That committee, made up of the chief engineer and plant, sales, and general managers, next decides which systems to keep, which to drop, and which to study further.

Sections 3 and 4 are self-explanatory, and are both aimed at eliminating equipment-related problems through further testing and by education of all personnel on equipment operations. Note that salespeople particularly are urged to go through the training process.

The next two parts cover installation procedures. Service workers are warned about environmental hazards that can affect different sensors. Such hazards include heat, static electricity, vibration, and electromagnetic interference from radio waves. The zoning section tells companies how they may set up their installations to isolate faults in different sensors and pieces of equipment.

Under subscriber education, firms are urged to inundate their customers with training films, brochures, seminars, and whatever else it takes to teach them how to operate their alarm systems properly.

The NBFAA also developed a separate booklet to educate alarm subscribers. It incorporates a discussion of alarm system fundamentals along with procedures that customers may undertake to reduce mistakes by their employees who operate the systems.

Last, the *False Alarm Handbook* asks alarm companies to work closely with the local police on this problem. Here, the NBFAA endorses companywide research and forming a local private security advisory council to oversee efforts.

Both the alarm company and the police must recognize that they need each other. Like surgeons and other medical specialists who need sophisticated drugs and instruments to prevent diseases, the law enforcement community needs the alarm industry. Prevention, the reason for alarm protection, must lead the war on crime.

At the same time, the alarm industry must remove from its ranks the flimflam-selling of placebos and faulty systems. Users must be taught to care for their security.

Police should take action against such companies and customers when they aggravate the false alarm problem. If some friendly arm-twisting fails to stop such practices, then police should meet with responsible alarm firms, and together they should develop programs and, if necessary, ordinances to penalize negligent subscribers and deceitful companies.

CONCLUSION

As we enter the 21st century and look back, we have seen a lot of changes occur, with many changes for the better. Passive infrared units are widely used and ultrasonic motion detectors are rarely used. Foil is no longer placed on glass windows being replaced by a properly placed PIR. Home and commercial applications of PIR units come in all shapes and sizes as well as all necessary patterns for proper coverage. Smoke detectors come with remote maintenance reporting to reduce false alarms (two-wire detectors only). Keypads are now hardware, and two-way voice modules and wireless and control panels (UL listed) are in single- and multizone panels.

The growth in technology will continue as will the need for updated technology.

GLOSSARY FOR ALARM SYSTEMS*

absorption The property of materials such as carpeting, drapes, acoustic ceilings, and so on, which causes them to soak up or deaden sound. The materials also deaden ultrasonics, so a higher than normal range setting may be required.

AC Abbreviation for alternating current.

access control 1. Any means of limiting entry into a building or area to those who are authorized. 2. A system that does this by use of coded cards, push button sequence, fingerprint comparison, hand geometry, retinal (eye) scans, or other means.

account A subscriber to an alarm company's services.

*From Trimmer, HW. Understanding and servicing alarm systems, 3rd ed. Boston, Butterworth-Heinemann 1981.

acoustic glass break sensors Can be installed on walls or ceilings. Detection is best when installed on a wall *opposite* protected glass, since sound waves need not then reflect off an opposing wall before reaching the detector.

active detector One that sends out or transmits energy in order to perform its detection function. Examples are ultrasonic, microwave, photoelectric beams, E-field fence detectors, and capacitance alarms.

air turbulence Air disturbance or churning caused by a breeze or draft from a fan, furnace, air conditioner, or other source. Air turbulence in the vicinity of an ultrasonic transducer can produce false alarms.

alarm condition The presence of a dangerous or undesired situation such as fire, intrusion, holdup, and so on, sensed and signaled by an alarm system.

alarm line A wire or telephone line used to report an alarm condition to a remote location such as a guard station or an alarm central office.

alarm signal An indication that some dangerous or unwanted condition is occurring, such as an intrusion, fire, holdup, and so on.

alarm system A collection of detection devices, control unit, annunciation/reporting equipment, control station(s), wiring, phone lines, radio channels, power supply, and other associated equipment connected together to detect and report the existence of an undesirable condition such as an intrusion, a fire, an unsafe condition in an industrial manufacturing process, and so on.

annunciator A device, typically a small horn or light, used to attract the attention of someone close by.

area protection 1. A detector that is sensitive over a two-dimensional space, such as a strain gauge sensor or a seismic detector. 2. A misnomer for **volumetric protection** (which is three-dimensional).

armed The condition of an alarm system when it is on, ready to be tripped when an intrusion is detected.

armed light A light or light-emitting diode, usually red, or other device that indicates the alarm system is armed or set.

audible alarm An alarm that makes noise (as opposed to a silent alarm) using a bell or horn.

audio alarm A detection device that is triggered upon detecting noises, such as the sounds of breaking and entering. See **audio discriminator**, **vault alarm, sonic detector**.

balanced magnetic contact See **high security magnetic contact**.

battery An assembly of two or more cells used to obtain higher voltages than that available from a single cell.

capacitance detector A device that detects an intruder's touching of or close approach to a protected metal object. Often used to protect safes and file cabinets. Protected objects must be metal, well insulated from the ground, and not too large. Also called safe alarm or proximity alarm. See **E-field detector**.

casement window A type of window that hinges outward and is usually opened with a crank. It is often difficult to mount contacts on casement windows. Tamper switches are sometimes used successfully.

central station 1. A central location where an alarm company monitors a large number of its own accounts. 2. A company that specializes in monitoring the alarm signals for many alarm companies for a fee.

certificated alarm system An alarm system that is installed by a UL-certified alarm company and that meets certain requirements for installation, service, and extent of coverage.

circuit breaker An electrical safety valve; a device designed to interrupt dangerously high currents. Unlike a fuse, a circuit breaker can be reset to be used again, thus no replacements are needed. Some circuit breakers can also be used as switches.

closed-circuit television (CCTV) An on premises TV system used to enable a guard to "watch" one or more critical areas such as entrances, high-value areas, and so on. The TV signal is used transmitted by coaxial cable or fiber optic cable and is usually limited to distances of a few hundred to a few thousand feet.

closing signal A signal transmitted by an alarm system to the central station when the proprietor (user) secures and leaves the premises at the close of business. Usually done on a prearranged time schedule.

coaxial cable A special kind of shielded cable that has one center conductor surrounded by relatively thick insulation, which in turn has

a shield (usually braided wires or sometimes spirally laid wires) over it. An outer plastic jacket is usually included. Used primarily for RF work such as antenna lead-in and for CCTV cameras.

commercial alarm An alarm installed in a commercial or business location, as opposed to a residential alarm.

day-night switch A switch located at the subscriber's premises used by the subscriber to signal the central station of opening and closing of the premises. Used only on direct-wire, supervised accounts (the milliamp signal method), and multiplex systems.

dedicated line or circuit A phone line or circuit that is dedicated solely to transmission of alarm signals. Examples are direct wire, McCulloh, multiplex, and derived channel.

door switch See **magnetic contact**.

Doppler shift The apparent frequency shift due to motion of an intruder in ultrasonic and microwave detection.

double-hung window A type of window popular in older construction. The lower sash (window) can be raised and the upper sash can be lowered. Two contacts are usually used to protect both sashes.

dry cell A type of battery that is not rechargeable. Dry cells are occasionally used in alarm work, but because of the required periodic replacement, rechargeable batteries are usually favored. (Rechargeable batteries also have to be replaced periodically, but not as often as dry cells.)

dual alarm service Protection of one premise by two separate alarm systems, usually serviced by different alarm companies. Thus protected, there is less likelihood that both systems could be successfully compromised and less chance of collusion among dishonest employees of the two alarm companies. Use is limited to high-risk applications because of the cost.

duress switch A special type of key switch that can be turned in either of two directions or can be operated with two different keys. One direction (or key) operates the alarm systems in a normal manner. The other direction (or key) signals the central station that the owner of the protected premises is under duress (i.e., has a gun in his back). By comparison, a holdup switch is activated secretly, whereas a duress switch is activated openly, and the burglar is unaware of its duress signaling function. (The burglar thinks it is a regular control switch.)

electronic siren An electronic device with speaker, used to simulate the sound of a motor-driven siren.

environmental considerations Factors that must be considered in the proper application of alarm detectors to reduce false alarms, particularly with motion sensors. Such factors include rain, fog, snow, wind, hail, humidity, temperature, corrosion, moving or swaying objects, vegetation growth, animals, and many others. They depend on the type(s) of detectors that is considered and where they are to be located.

exit–entry delay A feature of some alarm systems, particularly in residential applications, that permits locating the on/off station inside the protected premises. When exiting, the user turns the system on, which starts the exit time delay cycle (typically 30 to 120 seconds). He can then exit through a specific protected door without tripping the alarm during this delay. Later, when the user returns, the system is tripped when the specific door is opened. This action starts an entry delay cycle but does not cause an immediate alarm (although a small per-alert alarm may sound as a reminder). The user then has, typically, 15 to 60 seconds to turn the system off. An intruder would not have a key or would not know the secret code to turn the system off, therefore, the alarm would ring or a silent signal be transmitted after the entry delay expired.

holdup alarm A means of notifying a remote location, such as an alarm central station or police station, that a holdup is in progress. Holdup alarms are always silent and are actuated secretly, otherwise the noise of a local alarm or the obvious pushing of an alarm button could prompt the holdup man to acts of violence. A holdup alarm should not be confused with a panic alarm or with a duress alarm.

indicator light Any light, either incandescent or LED, which indicates the status of an alarm system, such as the "ready" light.

infrared detector 1. Passive type is one that detects an intruder by his body heat (which is infrared energy). This type does not emit any infrared energy, it only detects it. 2. Active type is a

photoelectric beam that uses infrared instead of visible light. This kind does emit infrared energy.

intrusion alarm An arrangement of electrical and/or electronic devices designed to detect the presence of an intruder or an attempt to break into a protected location, and to provide notification by making a loud noise locally (bell, siren, etc.) or by transmitting an alarm signal to some remote monitoring location or both.

key pad A collection of push buttons mounted on a plate, used to enter a secret code used to arm and disarm alarm systems. Often resembles a touchtone phone pad. Used to replace key-operated switches. Decoding of the correct combination is done by electronics mounted behind the pad. Also called a stand-alone key pad. Compare **system pad**.

line security The degree of protection of the alarm transmission path against compromise. Usually implies the application of additional measures to improve that security. See **line supervision**.

line supervision An arrangement where a known current, AC, DC, pulses, or a combination, is present on the line to the central station. Cutting or shorting the line will change this current, signaling an alarm. In high-security systems, complex line supervision systems are used to detect attempts to defeat the system.

line voltage 1. 120 V AC "house power." 2. The voltage on a telephone line used for alarm service.

magnetic contact A magnetically operated switch, typically used on doors and windows to detect opening. The switch is mounted on the frame or fixed part while the magnet is mounted on the movable door or window. Generally much easier to use than earlier, mechanically actuated switches. Available in NO, NC, or SPST contact forms.

mat switch A very thin, pressure-sensing switch placed under carpets (and carpet padding) to trip an alarm when an intruder steps on it. Typical size is 30×36 inches. Sizes vary from 7 inches to 24 inches. Typical thickness is 3/32 inch to 1/8 inch. Runner mat is 30 inches wide ×25 feet long and is cut to the desired length with scissors. With one exception, all mat switches are normally open. Supervised mats have two sets of leads. For damp or wet locations, sealed type mats should be used.

medical alert An alarm system by which an invalid, elderly, or sick person can push a button near his bedside to alert someone that a doctor, ambulance, or other medical assistance is required.

microprocessor A computer on a microchip, the heart of all personal computers. Now used as the heart of alarm control panels. With a microprocessor designed into a control, it is possible to obtain features that would be prohibitively expensive otherwise. Some examples are dozens of zones, information displays in English (or other language), and zone parameters (e.g., speed of response, perimeter/interior/entry–exit/instant response, etc.) assignable for each zone. Most important, these features can be changed, often without requiring a service call to the premises. First introduced by Ron Gottsegen of Radionics in 1977.

microwave detector A device that senses the motion of an intruder (and of other things) in a protected area by a Doppler shift in the transmitted RF energy. Microwave detectors generally operate at 10.525 GHz. Older units operated at 915 MHz. Both have largely been replaced by PIR detectors, which are less susceptible to false alarms.

money trap A special switch placed in the bottom of a cash drawer. It is activated during a holdup by pulling out the bottom bill of the stack, which has been previously inserted into a trap. To prevent a false alarm, care must be taken not to remove that bottom bill at any other time.

motion detector Any of several devices that detects an intruder by his motion within a protected area or protected volume. See **ultrasonic**, **microwave**, **passive IR**, **area protection**, and **volumetric protection.**

multiplex 1. In general, any method of sending many signals over one communications channel. 2. Specifically, any method of sending alarm signals from many subscribers over one pair of wires to a monitoring location. (Technically, a McCulloh circuit does this, but the term multiplex is generally used to refer to the newer, electronic techniques using polling computers and similar methods.)

open and closed loop A combination of an open loop and a closed loop, used on some controls. Note that, unlike the double closed loop, the open loop conductor in this system is not

supervised. That is, cutting this wire will disable part of the system without causing an alarm condition.

opening 1. Any possible point of entry for an intruder, such as windows, doors, ventilators, roof hatches, and so on. 2. Any such point that is protected by an alarm detection device. 3. See **opening signal**. 4. See **scheduled opening** and **unscheduled opening**.

panic alarm A local bell alarm, triggered manually, usually by pushing a button (as opposed to being tripped by some kind of detection device). Usually found only in residential systems. The panic button permits the owner/subscriber to trigger the alarm manually in case of intrusion, even though the alarm system happens to be turned off at the time. A panic alarm (which is audible) should not be confused with a holdup alarm, which is always silent.

power supply Any source of electrical energy. More specifically, power supply usually refers to an electronic device that converts AC to DC for use by alarm equipment. It may also reduce the voltage from 120 V to the voltage needed by the alarm equipment. Some power supplies have provision for connecting a standby battery. Others will accommodate a rechargeable battery and will provide the necessary charging current for that battery.

preventive maintenance Testing and checking out alarm systems on a regularly scheduled basis to locate and repair potential problems before false alarms or system failures result. Unfortunately, preventive maintenance is usually forgotten until trouble occurs.

reversing relay 1. A method of transmitting an alarm signal over a telephone wire by reversing the DC polarity. In the secure mode, a voltage is sent over the phone line from the protected premises to the monitoring location to provide line supervision. An alarm signal is transmitted by reversing the polarity, usually by operating a DPDT relay in the subscriber's control. 2. The relay used to reverse the polarity.

shunt switch A key-operated switch located outside the protected premises that allows the subscriber to bypass usually just one door to permit entry without tripping the alarm system. He will normally proceed to the control or transmitter to turn off the entire system with the on/off switch, usually using the same key. Upon closing the premises, the procedure is reversed.

silent alarm An alarm system that does not ring a bell or give any other indication of an alarm condition at the protected premises; instead it transmits an alarm signal to an alarm central station or other monitoring location.

siren 1. Traditionally, a motor-driven noisemaker used on police cars, fire trucks, ambulances, and so on. 2. An electronic replacement for (1) that produces a very similar sound.

sonic detector 1. A Doppler-principle detection device much like ultrasonic except that is uses an audible frequency. Not very common. 2. A misnomer for ultrasonic.

subscriber error A false or loss of alarm protection caused by the subscriber not following the correct procedures in the use of the alarm system.

switch A mechanically or magnetically operated device used to open and close electrical circuits.

tamper-proof box This term is somewhat of a misnomer because few things are "proof" against attack. The term is usually used to indicate that a control, bell, or equipment box is equipped with a tamper switch to signal an alarm when the door is opened. Tamper switches are preferably connected to a 24-hour protective circuit. Bell boxes or other boxes outside the protected area should also be equipped with a double door. Opening the outer door triggers the tamper switch, while the inner door denies the attacker immediate access to the bell or its wiring.

transmitter 1. A device that sends an alarm signal to a remote point, such as a McCulloh transmitter. 2. The unit at the end of a photoelectric beam that sends out the light or invisible infrared energy. 3. The ultrasonic transducer that sends out the ultrasonic energy.

UL-listed alarm company An alarm company that meets the requirements of Underwriters' Laboratories and is so designated by appearing on UL's published list.

UL standard for alarms Underwriters' Laboratories publishes many standards outlining the requirements that must be met by alarm equipment/alarm companies in order to obtain UL listing. The most important of these is UL 681, which outlines alarm system

installation requirements. Many others cover various kinds of equipment. It is important to bear in mind that there are many UL listings for many UL standards, many of which are unrelated to security (such as electrical safety). Therefore, the term UL listed is meaningless unless the exact nature of the "list" is detailed. UL 639 outlines transient protection requirements. UL 611 outlines central station units and systems.

ultrasonic detector A device that senses motion of an intruder (and of other things) in a protected area by a Doppler shift in the transmitted ultrasonic energy (sound is too high a frequency to be heard by humans). Rarely used anymore.

unscheduled opening Opening of a protected premise at an unscheduled time, that is, not a scheduled opening time. For a silent alarm, supervised account subscribers notify the monitoring alarm company in advance of their standard opening (and closing) times. If the owner or authorized person wishes to enter at any other time, he has to make special arrangements with the alarm company by phone and prearranged secret code word or, preferably, by letter.

vault alarm An alarm system used to protect a vault such as a bank vault or storage vault. This is a special type of audio alarm and usually has a test feature via the ring-back circuit, which can be actuated from the alarm central station.

walk test A procedure of actually walking through the area protected by a motion detector to determine the actual limits of its coverage. Indication is usually provided by an LED mounted on the detection unit. This indicator should be disabled or covered when not used for walk-testing. This will prevent a would-be burglar from doing his own walk-testing during open-for-business hours to determine holes in the coverage.

zone Large protected premises are divided into areas or zones, each having its own indicator or annunciator. This helps pinpoint the specific area of intrusion and is a great aid in narrowing down a problem when troubleshooting. Today's control units may have 16, 30, 48, or more zones.

zone light A light, LED, or other device used to indicate the status of each zone in a multiple-zone system. One or more indicators can be provided per zone to indicate any of the following: ready, armed, alarmed, and zoned-out.

APPENDIX 11.A SMOKE DETECTORS

The following was extracted from 3/6/2002: GE Interlogix eCommunity message addresses a common question regarding smoke sensors. For information on ESL fire and safety products, visit http://www.sentrol.com/products/firesafety.asp. The question and answer are provided courtesy of the Moore-Wilson Signaling Report (vol. 9, no. 5), a publication of Hughes Associates, Inc. For subscription information, email tm-wsr@haifire.com.

Q: I have heard a lot of controversial comments about the use of ionization-type smoke detectors versus photoelectric-type smoke detectors. Where would one specifically choose to use ionization-type smoke detectors?

A: Proper selection of a type of detector begins with an understanding of the operating principles of each type of detector.

In an ionization smoke detector, "a small amount of radioactive material is used to ionize the air between two differently charged electrodes to sense the presence of particles. Smoke particles entering the ionization volume decrease the conductance of the air by reducing ion mobility. The reduced conductance signal is processed and used to convey an alarm condition when it meets present criteria."

In a photoelectric light-scattering detector, "a light source and photosensitive sensor arranged so that the rays from the light source do not normally fall onto the photosensitive sensor. Then smoke particles enter the light path; some of the light is scattered reflection and refraction onto the sensor. The light signal is processed and used to convey an alarm condition when it meets preset criteria."

The appendix further explains that photoelectric light-scattering detectors respond more to visible particles, larger than 1 μ in size, produced by most smoldering fires. They respond somewhat less to the smaller particles typically produced by flaming fires. They also respond less to fires yielding black or darker smoke, such as fires involving plastics and rubber tires.

Ionization detectors tend to exhibit somewhat opposite characteristics. In a fire yielding "invisible" particles of a size less than 1 μ, an ionization detector will more likely respond than will a photoelectric light-scattering detector. Particles of this size tend to more readily result from flaming fires. Fuel in flaming fires burns "cleaner," producing smaller particles.

Thus, the answer to whether you should use one type of detector over another lies in understanding the burning characteristics of the particular fuel. An ionization-type smoke detector will likely detect a fire that produces flaming combustion more quickly, and a photoelectric-type detector will likely detect a low energy fire that produces larger particles during combustion more quickly.

Finally, keep in mind that both types of smoke detectors successfully pass the same battery of tests at the nationally recognized testing laboratories. For example, UL-listed ionization smoke detectors and UL-listed photoelectric smoke detectors pass the same tests under UL 268, Standard for Safety for Smoke Detectors for Fire Protection Signaling Systems.

APPENDIX 11.B ALARM CERTIFICATE SERVICES GLOSSARY OF TERMS CERTIFICATE TYPES

The Fire Alarm System Certificate Types are

- Central Station (NFPA 71 or 72)—Central Station Fire Alarm System Certificate
- Local (NFPA 72)—Local Fire Alarm System Certificate
- Auxiliary (NFPA 72)—Auxiliary Fire Alarm System Certificate
- Remote Station (NFPA 72)—Remote Station Fire Alarm System Certificate
- Proprietary (NFPA 72)—Proprietary Fire Alarm System Certificate

The Burglar Alarm System Certificate Types are

- Central Station—Central Station Burglar Alarm System Certificate
- Mercantile—Mercantile Burglar Alarm System Certificate
- Bank—Bank Burglar Alarm System Certificate
- Proprietary—Proprietary Burglar Alarm System Certificate
- Residential—Residential Burglar Alarm System Certificate
- National Industrial Security—National Industrial Security System Certificate

DEFINITIONS

alarm service company—The listed company responsible for maintaining the alarm system under UL's Certificate Service programs.

alarm system—A fire alarm signaling system that is considered to be the combination of interrelated signal initiating devices, signal transmitting devices, signal notification devices, and control equipment and interconnecting wiring installed for a particular application.

category control number (CNN)—An alphanumeric system used by UL to designate and identify the individual grouping of products that have common functional and/or design features to facilitate the application of uniform requirements as the basis of UL Listing, Classification, Recognition, or Certificate Service.

coverage—A term that identifies the extent of coverage provided by automatic fire detectors.

total coverage— Detectors are installed in all areas, rooms, and spaces, as defined in NFPA 72 (National Fire Alarm Code).

selected area coverage—Same as total coverage but only for a specified area(s) of the protected property.

partial coverage—Deviations from total or selected coverage. Number of devices and their locations are specified.

file number—Alarm service company's file number. A number assigned by UL to identify a file for a listee within a specific product category.

protected property—The alarm user, business, residence, location, and/or area protected by the alarm system.

runner—A person other than the required number of operators on duty at a central, supervising, or runner station (or otherwise in contact with these stations) available for prompt dispatching, when necessary, to the protected premises.

service center number—A number, code, or distinctive identification, assigned either by the listee or UL, which when used in association with a client's file number uniquely defines a central station, service center, satellite station, monitoring station, or other service location of the listee.

standard—Criteria used by UL as the primary basis for determining the eligibility of a product to use the UL's Listing, Classification, or Recognition Mark and other markings or certificates that may be required.

STANDARDS

- UL 681—Installation and Classification of Burglar and Holdup-Alarm Systems
- UL 827—Central Station Alarm Services
- UL 1023—Household Burglar-Alarm System Units
- UL 1076—Proprietary Burglar-Alarm Units and Systems
- UL 1641—Installation and Classification of Residential Burglar-Alarm Systems
- UL 1981—Central Station Automation Systems
- UL 2050—National Industrial Security Systems for the protection of Classified Materials
- NFPA 71—Standard for the Installation, Maintenance, and Use of Signaling Systems for Central Station Service
- NFPA 72—Standard for the Installation, Maintenance, and Use of Protective Signaling Systems. (1990)

APPENDIX 11.C FIRE CLASSIFICATIONS

A fire is very dangerous, but it can be even more so if the wrong equipment is used in fighting it. Because of this, a fire classification system has been established that has made it easy to match the correct fire extinguisher to the correct type of fire.

Fires are divided into five types. It is important to use the correct fire extinguisher in combating the blaze. The five classifications include:

1. **Class A:** This fire is distinguishable by the fact that it leaves an ash. Some of the materials that burn in a Class A fire are wood, cloth, leaves, and rubbish (e.g., this is the class of fire that people have in their fireplaces).
2. **Class B:** This fire is ignited by flammable liquids. Examples are gasoline, oil, and lighter fluid (e.g., a charcoal grill is started by Class B fires).
3. **Class C:** These are electrical fires. They are common in fuse boxes.
4. **Class D:** Metals that are flammable cause Class D fires. Examples are sodium, magnesium, and potassium.
5. **Class K:** In recent years studies have found that some cooking oils produce too much heat to be controlled and extinguished by traditional Class B extinguishing agents. Class K fires and extinguishers deal with cooking oil fires.

USE OF FIRE EXTINGUISHERS

When combating a fire, the extinguisher used must be the same class as the fire. If a Class A extinguisher is used to put out a Class C fire, it could cause an explosion if the electrical current is still flowing. The following is an explanation of the contents and purposes of each type of extinguisher.

- **Class A Extinguishers** will put out fires in ordinary combustibles, such as wood and paper. The numerical rating for this class of fire extinguisher refers to the amount of water the fire extinguisher holds and the amount of fire it will extinguish.
- **Class B Extinguishers** should be used on fires involving flammable liquids, such as grease, gasoline, oil, and so forth. The numerical rating for this class of fire extinguisher states the approximate number of square feet of a flammable liquid fire that a nonexpert can expect to extinguish.

- **Class C Extinguishers** are suitable for use on electrically energized fires. This class of fire extinguishers does not have a numerical rating. The presence of the letter C indicates that the extinguishing agent is nonconductive.
- **Class D Extinguishers** are designed for use on flammable metals and are often specific for the type of metal in question. There is no picture designator for Class D extinguishers. These extinguishers generally have no rating and there is no multipurpose rating for use on other types of fires.
- **Class K extinguishers** are suitable for cooking oil fires. Studies have found that some cooking oils produce too much heat to be controlled and extinguished by traditional Class B extinguishing agents. Class K extinguishers are a polished stainless steel cylinder, and these wet chemical extinguishers are the best restaurant kitchen appliance hand-portable fire extinguishers you can purchase. At Computershare we have such units in the kitchen.

CHAPTER

11

Video Technology Overview*

Herman Kruegle

OVERVIEW

The second half of the 2000s witnessed a quantum jump in video security technology. This technology has manifested with a new generation of video components, such as digital cameras, multiplexers, DVRs, and so forth. A second significant activity has been the integration of security systems with computer-based local area networks (LANs), wide area networks (WANs), wireless networks (WiFi), intranets, and Internet and the World Wide Web (WWW) communications systems.

Although today's video security system hardware is based on new technology that takes advantage of the great advances in microprocessor computing power, solid-state and magnetic memory, digital processing, and wired and wireless video signal transmission (analog, digital over the Internet, etc.), the basic video system still requires the lens, camera, transmission medium (wired cable, wireless), monitor, recorder, and so forth. This chapter describes current video security system components and is an introduction to their operation.

The primary function of any video security or safety system is to provide remote eyes for the security force located at a central control console or remote site. The video system includes the illumination source, the scene to be viewed, the camera lens, the camera, and the means of transmission to the remote monitoring and recording equipment. Other equipment often necessary to complete the system includes video switchers, multiplexers, video motion detectors (VMDs), housings, scene combiners and splitters, and character generators.

This chapter describes the technology used to (1) capture the visual image, (2) convert it to a video signal, (3) transmit the signal to a receiver at a remote location, (4) display the image on a video monitor, and (5) record and print it for permanent record. Figure 11-1 shows the simplest video application requiring only one video camera and monitor.

The printer and video recorder are optional. The camera may be used to monitor employees, visitors, or people entering or leaving a building. The camera could be located in the lobby ceiling and pointed at the reception area, the front door, or an internal access door. The monitor might be located hundreds or thousands of feet away, in another building or another city or country with the security personnel viewing that same lobby, front door, or reception area. The video camera/monitor system effectively extends the eyes, reaching from observer location to the observed location.

*Originally from Kruegle, H. CCTV surveillance. Boston: Butterworth-Heinemann, 2006. Updated by the editor, Elsevier, 2011.

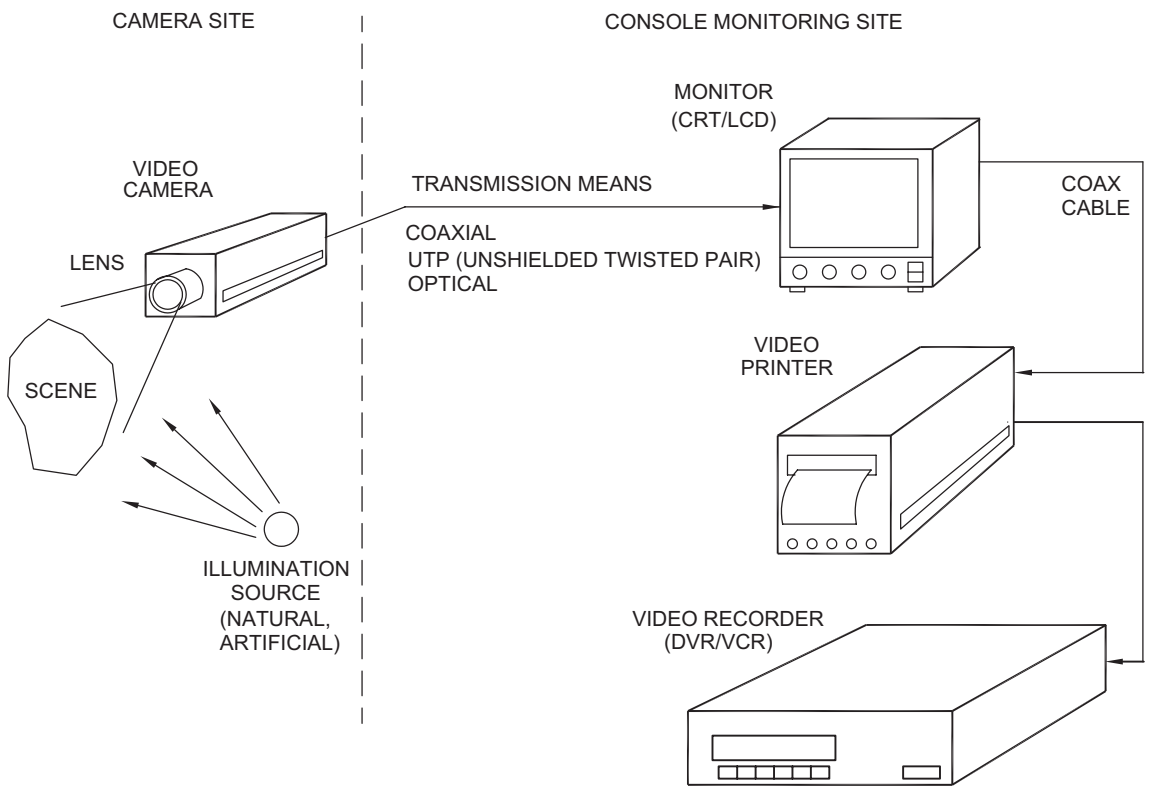


FIGURE 11-1 Single-camera video system.

The basic one-camera system shown in Figure 11-1 includes the following hardware components.

- **Lens.** Light from the illumination source reflects off the scene. The lens collects the light from the scene and forms an image of the scene on the light-sensitive camera sensor.
- **Camera.** The camera sensor converts the visible scene formed by the lens into an electrical signal suitable for transmission to the remote monitor, recorder, and printer.
- **Transmission link.** The transmission media carries the electrical video signal from the camera to the remote monitor. Hard-wired media choices include: (a) coaxial, (b) two-wire unshielded twisted-pair (UTP), (c) fiber optic cable, (d) LAN, (e) WAN, (f) intranet, and (g) Internet network. Wireless choices include: (a) radio frequency (RF), (b) microwave, or (c) optical infrared (IR). Signals can be analog or digital.
- **Monitor.** The video monitor or computer screens (CRT, LCD, or plasma) display the camera image by converting the electrical video signal back into a visible image on the monitor screen.
- **Recorder.** The camera scene is permanently recorded by a real-time or time lapse (TL) VCR onto a magnetic tape cassette or by a DVR using a magnetic disk hard drive.
- **Hard-copy printer.** The video printer produces a hard-copy paper printout of any live or recorded video image, using thermal, inkjet, laser, or other printing technology.

The first four components are required to make a simple video system work. The recorder and/or printer is required if a permanent record is required.

Figure 11-2 shows a block diagram of a multicamera analog video security system using

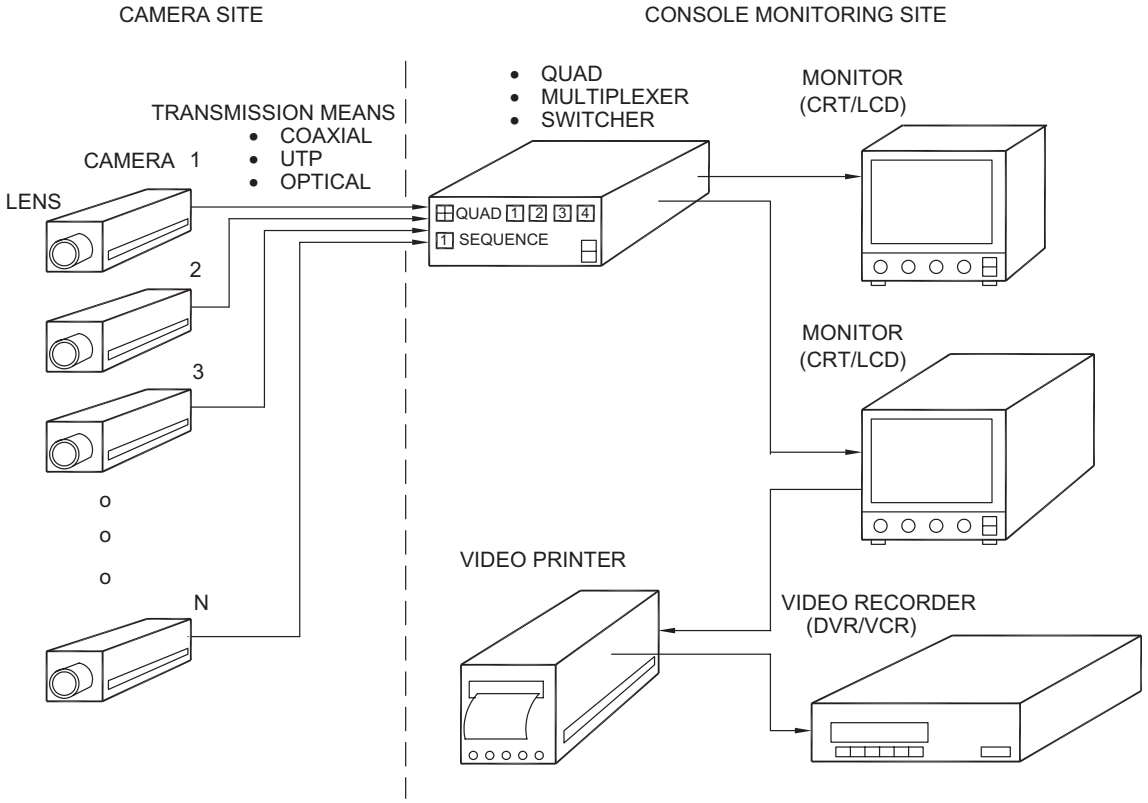


FIGURE 11-2 Comprehensive video security system.

these components plus additional hardware and options to expand the capability of the single-camera system to multiple cameras, monitors, recorders, and so forth, providing a more complex video security system.

Additional ancillary supporting equipment for more complex systems includes: camera switchers, quads, multiplexers, environmental camera housings, camera pan/tilt mechanisms, image combiners and splitters, and scene annotators.

- **Camera switcher, quad, multiplexer.** When a closed-circuit TV (CCTV) security system has multiple cameras, an electronic switcher, quad, or multiplexer is used to select different cameras automatically or manually to display the images on a single or multiple monitors, as individual or multiple scenes. The quad can digitally combine four cameras. The multiplexer can digitally combine 4, 9, 16, or even 32 separate cameras.
- **Housings.** The many varieties of camera/lens housings fall into three categories: indoor, outdoor, and integral camera/housing assemblies. Indoor housings protect the camera and lens from tampering and are usually constructed from lightweight materials. Outdoor housings protect the camera and lens from the environment such as precipitation, extremes of heat and cold, dust, dirt, and vandalism.
- **Dome housing.** The dome camera housing uses a hemispherical clear or tinted plastic dome enclosing a fixed camera or a camera with pan/tilt and zoom lens capability.
- **Plug and play camera/housing combination.** To simplify surveillance camera installations many manufacturers are now packaging the camera-lens-housing as a complete assembly.

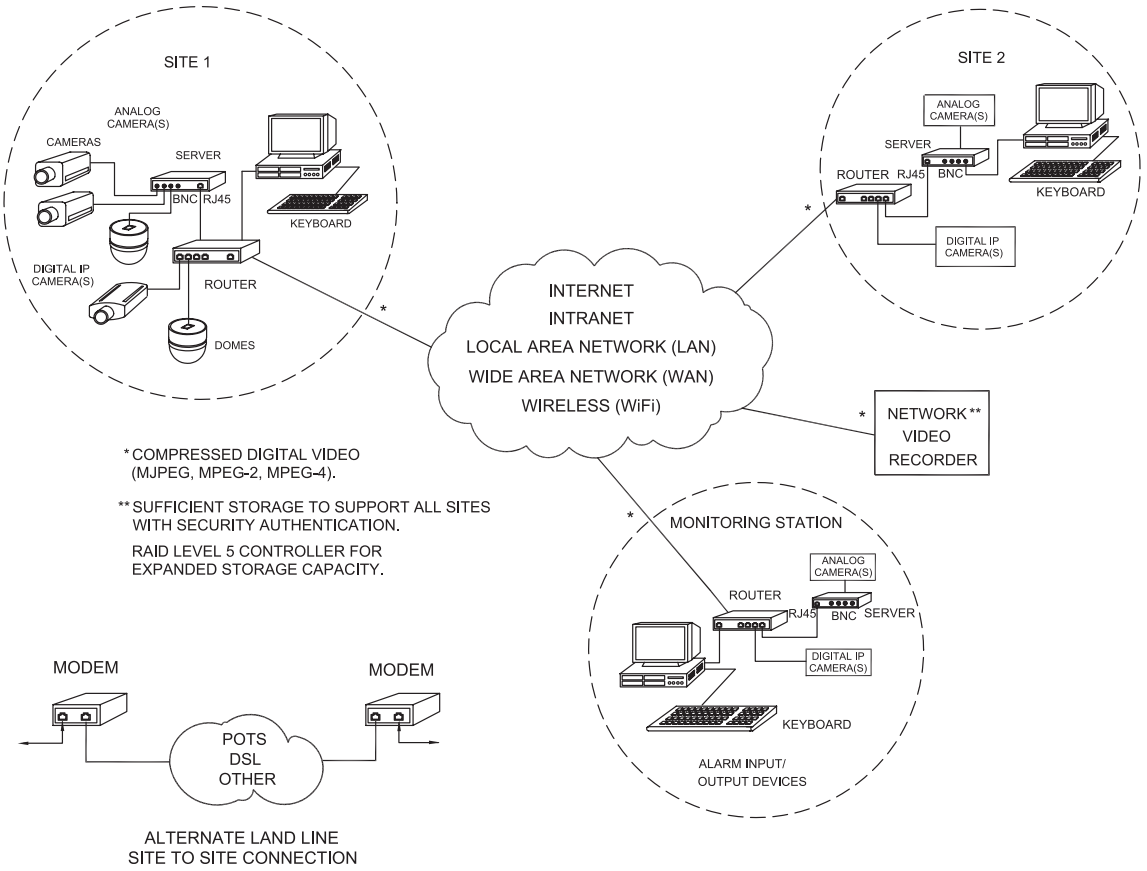


FIGURE 11-3 Networked digital video system block diagram.

These plug-and-play cameras are ready to mount in a wall or ceiling and to connect the power in and the video out.

- **Pan/tilt mechanism.** When a camera must view a large area, a pan and tilt mount is used to rotate it horizontally (panning) and to tilt it, providing a large angular coverage.
- **Splitter/combiner/inserter.** An optical or electronic image combiner or splitter is used to display more than one camera scene on a single monitor.
- **Annotator.** A time and date generator annotates the video scene with chronological information. A camera identifier puts a camera number (or name such as Front Door, etc.) on the monitor screen to identify the scene displayed by the camera.

The digital video surveillance system includes most of the devices in the analog video system. The primary differences manifest in using digital electronics and digital processing within the video devices. Digital video components use digital signal processing (DSP), digital video signal compression, digital transmission, recording, and viewing. Figure 11-3 illustrates these devices and signal paths and the overall system block diagram for the digital video system.

VIDEO SYSTEM

Figure 11-4 shows the essentials of the CCTV camera environment: illumination source, camera, lens, and the camera–lens combined field of view (FOV), that is, the scene the camera–lens combination sees.

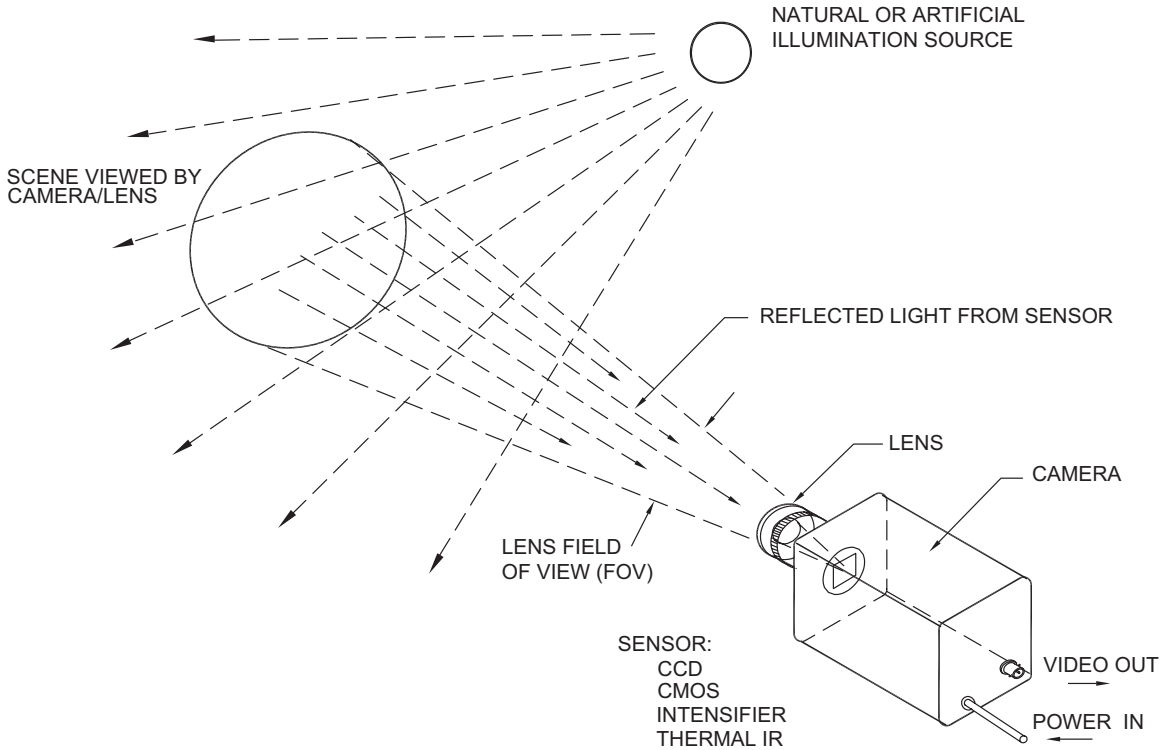


FIGURE 11-4 Video camera, scene, and source illumination.

The Role of Light and Reflection

A scene or target area to be viewed is illuminated by natural or artificial light sources. Natural sources include the sun, the moon (reflected sunlight), and starlight. Artificial sources include incandescent, sodium, metal arc, mercury, fluorescent, infrared, and other man-made lights.

The camera lens receives the light reflected from the scene. Depending on the scene to be viewed the amount of light reflected from objects in the scene can vary from 5 or 10% to 80 or 90% of the light incident on the scene. Typical values of reflected light for normal scenes such as foliage, automobiles, personnel, and streets fall in the range of about 25–65%. Snow-covered scenes may reach 90%.

The amount of light received by the lens is a function of the brightness of the light source, the reflectivity of the scene, and the transmission characteristics of the intervening atmosphere. In outdoor applications there is usually a considerable optical path from the source to the scene and back to the camera; therefore, the transmission through the atmosphere must be considered. When atmospheric conditions are clear, there is generally little or no attenuation of the reflected light from the scene. However, when there is precipitation (rain, snow, or sleet, or when fog intervenes) or in dusty, smoky, or sand-blown environments, this attenuation might be substantial and must be considered. Likewise in hot climates thermal effects (heat waves) and humidity can cause severe attenuation and/or distortion of the scene. Complete attenuation of the reflected light from the scene (zero visibility) can occur, in which case no scene image is formed.

Since most solid-state cameras operate in the visible and near-IR wavelength region the general rule of thumb with respect to visibility is that if the human eye cannot see the scene neither can

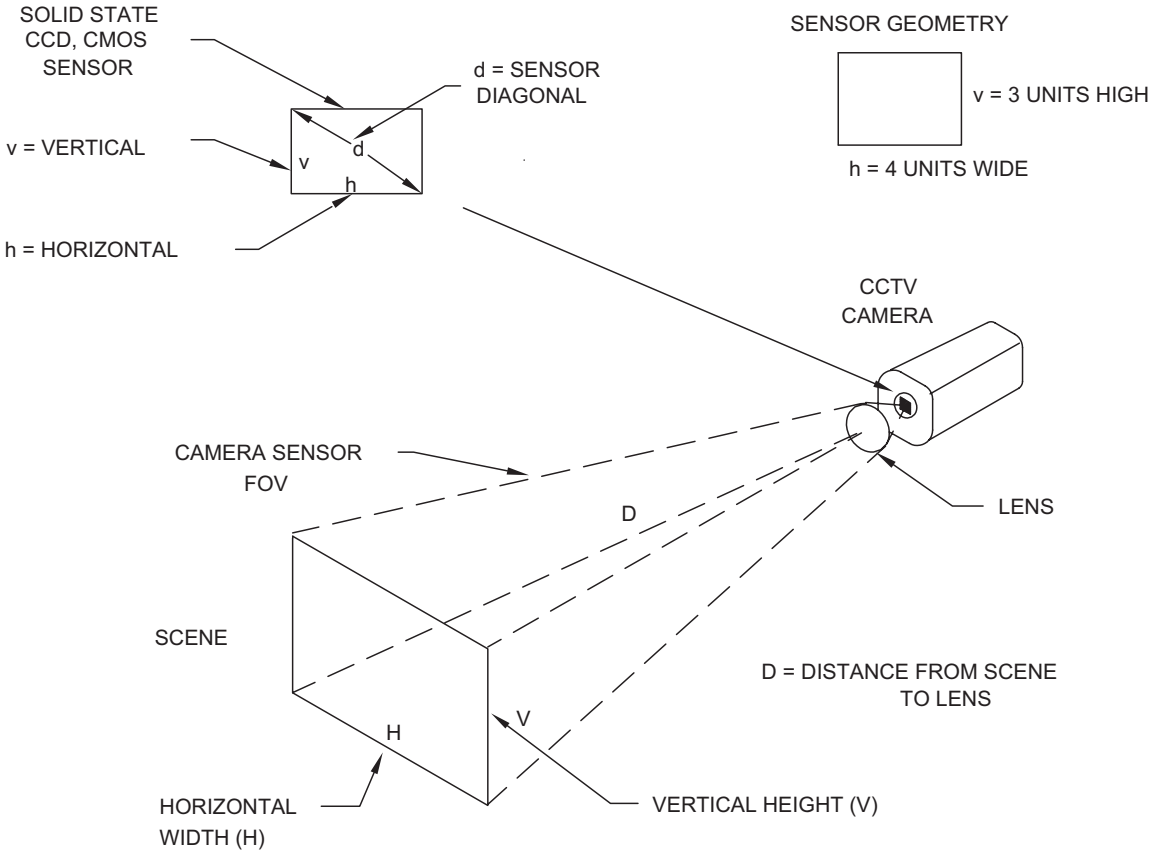


FIGURE 11-5 Video scene and sensor geometry.

the camera. Under this situation, no amount of increased lighting will help; however, if the visible light can be filtered out of the scene and only the IR portion used, scene visibility might be increased somewhat.

This problem can often be overcome by using a thermal IR imaging camera that works outside of the visible wavelength range. These thermal IR cameras produce a monochrome display with reduced image quality and are much more expensive than the charge-coupled device (CCD) or complementary metal oxide semiconductor (CMOS) cameras. Figure 11-5 illustrates the relationship between the viewed scene and the scene image on the camera sensor.

The lens located on the camera forms an image of the scene and focuses it onto the sensor. Almost all video systems used in security systems have a 4 × 3 aspect ratio (4 units wide × 3 units high) for both the image sensor and the field of view. The width parameter is designated as h, and H, and the vertical as v, and V. Some cameras have a 16 × 9 units high definition television (HDTV) format.

Lens Function

The camera lens is analogous to the lens of the human eye (Figure 11-6) and collects the reflected radiation from the scene much like the lens of your eye or a film camera. The function of the lens is to collect reflected light from the scene and focus it into an image onto the CCTV camera sensor. A fraction of the light reaching the scene from the natural or artificial

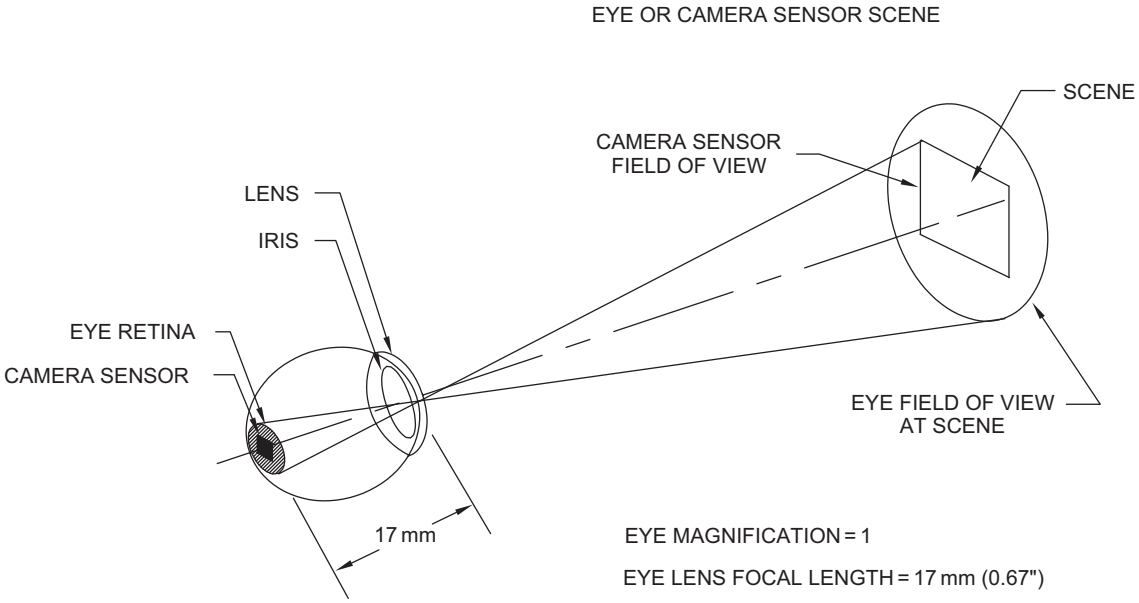


FIGURE 11-6 Comparing the human eye to the video camera lens.

illumination source is reflected toward the camera and intercepted and collected by the camera lens. As a general rule, the larger the lens diameter, the more light will be gathered, the brighter the image on the sensor, and the better the final image on the monitor. This is why larger aperture (diameter) lenses, having a higher optical throughput, are better (and more expensive) than smaller diameter lenses that collect less light. Under good lighting conditions—bright indoor lighting, outdoors under sunlight—the large-aperture lenses are not required and there is sufficient light to form a bright image on the sensor by using small-diameter lenses.

Most video applications use a fixed-focal-length (FFL) lens. The FFL lens, like the human eye lens, covers a constant angular FOV. The FFL lens images a scene with constant *fixed* magnification. A large variety of CCTV camera lenses are available with different focal lengths (FLs) that provide different FOVs. Wide-angle, medium-angle, and narrow-angle (telephoto) lenses produce different magnifications and FOVs. Zoom and varifocal lenses can be adjusted to have variable FLs and FOVs.

Most CCTV lenses have an iris diaphragm (as does the human eye) to adjust the open area of the lens and change the amount of light passing through it and reaching the sensor. Depending on the application, manual- or automatic-iris lenses are used.

In an automatic-iris CCTV lens, as in a human eye lens, the iris closes automatically when the illumination is too high and opens automatically when it is too low, maintaining the optimum illumination on the sensor at all times. Figure 11-7 shows representative samples of CCTV lenses, including FFL, varifocal, zoom, pinhole, and a large catadioptric lens for long-range outdoor use (which combines both mirror and glass optical elements).

CAMERA FUNCTION

The lens focuses the scene onto the camera image sensor, which acts like the retina of the eye or the film in a photographic camera. The video camera sensor and electronics convert the visible image into an equivalent electrical signal suitable for transmission to a remote monitor.

FIGURE 11-7 Representative video lenses.

Figure 11-8 is a block diagram of a typical analog CCTV camera.

The camera converts the optical image produced by the lens into a time-varying electric signal that changes (modulates) in accordance with the light-intensity distribution throughout the scene. Other camera electronic circuits produce synchronizing pulses so that the time-varying video signal can later be displayed on a monitor or recorder or printed out as hard copy on a video printer. While cameras may differ in size and shape depending on specific type and capability, the scanning process used by most cameras is essentially the same. Almost all cameras must scan the scene, point by point, as a function of time. (An exception is the image intensifier.) Solid-state CCD or CMOS color and monochrome cameras are used in most applications. In scenes with low illumination, sensitive CCD cameras with IR illuminators are used. In scenes

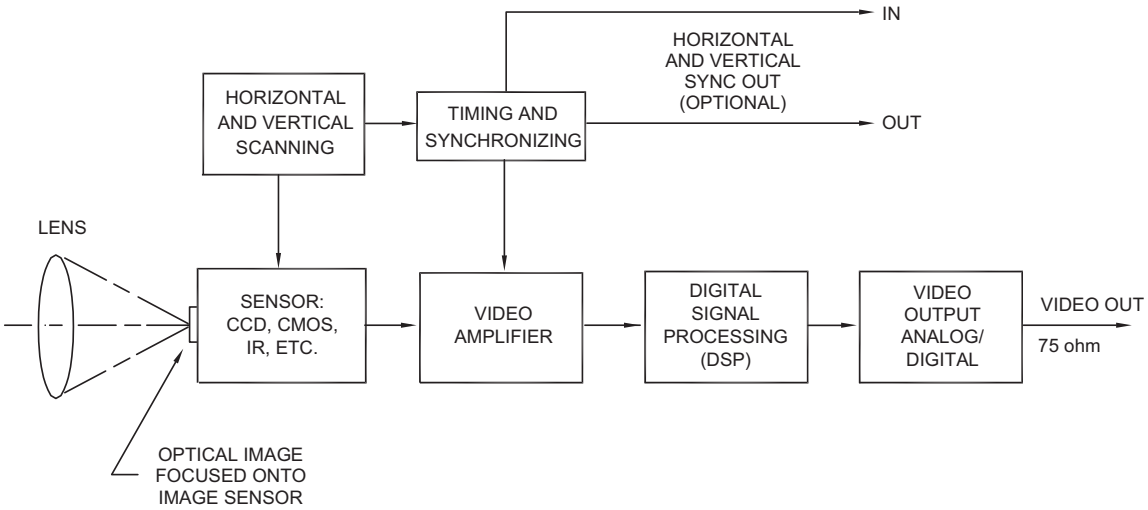


FIGURE 11-8 Analog CCTV camera block diagram.

with very low illumination and where no active illumination is permitted (i.e., covert) low-light-level (LLL) intensified CCD (ICCD) cameras are used. These cameras are complex and expensive.

Figure 11-9 shows a block diagram of an analog camera with (a) DSP and (b) the all-digital Internet Protocol (IP) video camera.

In the early 1990s, the nonbroadcast, tube-type color cameras available for security applications lacked long-term stability, sensitivity, and high resolution. Color cameras weren't used much in security applications until solid-state color CCTV cameras became available through the development of solid-state color sensor technology and widespread use of consumer color CCD cameras used in camcorders. Color cameras have now become standard in security systems and most CCTV security cameras in use today are color. Figure 11-10 shows representative CCTV cameras including monochrome and color solid-state CCD and CMOS cameras, a small single board camera, and a miniature remote head camera.

Transmission Function

Once the camera has generated an electrical video signal representing the scene image, the signal is transmitted to a remote security monitoring site via some transmission means: coaxial cable, two-wire twisted-pair, LAN, WAN, intranet, Internet, fiber optic, or wireless techniques. The choice of transmission medium depends on factors such as distance, environment, and facility layout.

If the distance between the camera and the monitor is short (10–500 feet), coaxial cable, UTP, and fiber optic or wireless is used. For longer distances (500 feet to several thousand feet) or where there are electrical disturbances, fiber optic cable and UTP are preferred. For very long distances and in harsh environments (frequent lightning storms) or between separated buildings where no electrical grounding between buildings is in place, fiber optics is the choice. In applications where the camera and monitor are separated by roadways or where there is no right of way, wireless systems using RF, microwave, or optical transmission are used. For transmission over many miles or from city to city the only choice is the digital or Internet IP camera using compression techniques and transmitting over the Internet. Images from these Internet systems are not real time but sometimes come close to real time.

Monitor Function

At the monitoring site a cathode ray tube (CRT) or LCD or plasma monitor converts the video signal back into a visual image on the monitor face via electronic circuitry similar but inverse to that in the camera.

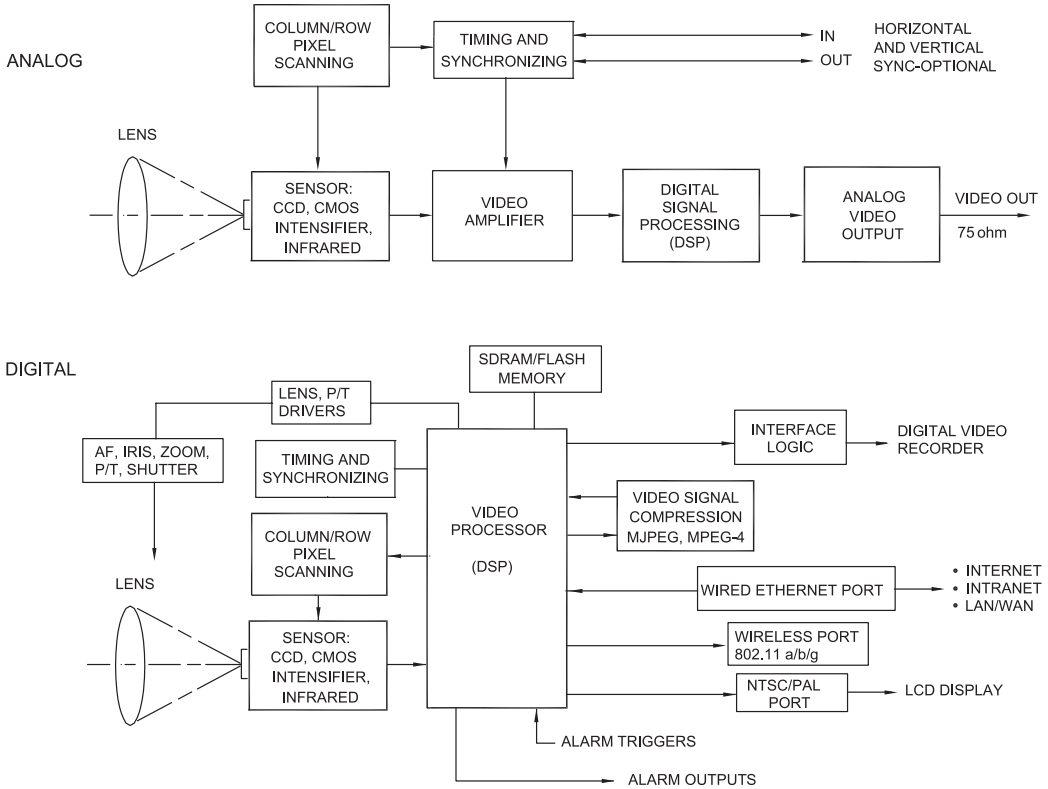


FIGURE 11-9 Analog camera with DSP and all-digital camera block diagram.

The final scene is produced by a scanning electron beam in the CRT in the video monitor. This beam activates the phosphor on the CRT, producing a representation of the original image onto the faceplate of the monitor. Alternatively, the video image is displayed point by point on an LCD or plasma screen. A permanent record of the monitor video image is made using a VCR tape or DVR hard disk magnetic recorder and a permanent hard copy is printed with a video printer.

Recording Function

For decades the VCR has been used to record monochrome and color video images. The real-time and TL VCR magnetic tape systems have been a reliable and efficient means for recording security scenes.

Beginning in the mid-1990s the DVR was developed using a computer hard disk drive and digital electronics to provide video image recording. The availability of large memory disks (hundreds of megabytes) made these machines available for long-duration security recording. Significant advantages of the DVR over the VCR are the high reliability of the disk as compared with the cassette tape, its ability to perform high-speed searches (retrieval of images) anywhere on the disk, and absence of image deterioration after many copies are made.

SCENE ILLUMINATION

A scene is illuminated by either natural or artificial illumination. Monochrome cameras can operate with any type of light source. Color cameras need light that contains all the colors in the visible spectrum and light with a reasonable balance of all the colors to produce a satisfactory color image.

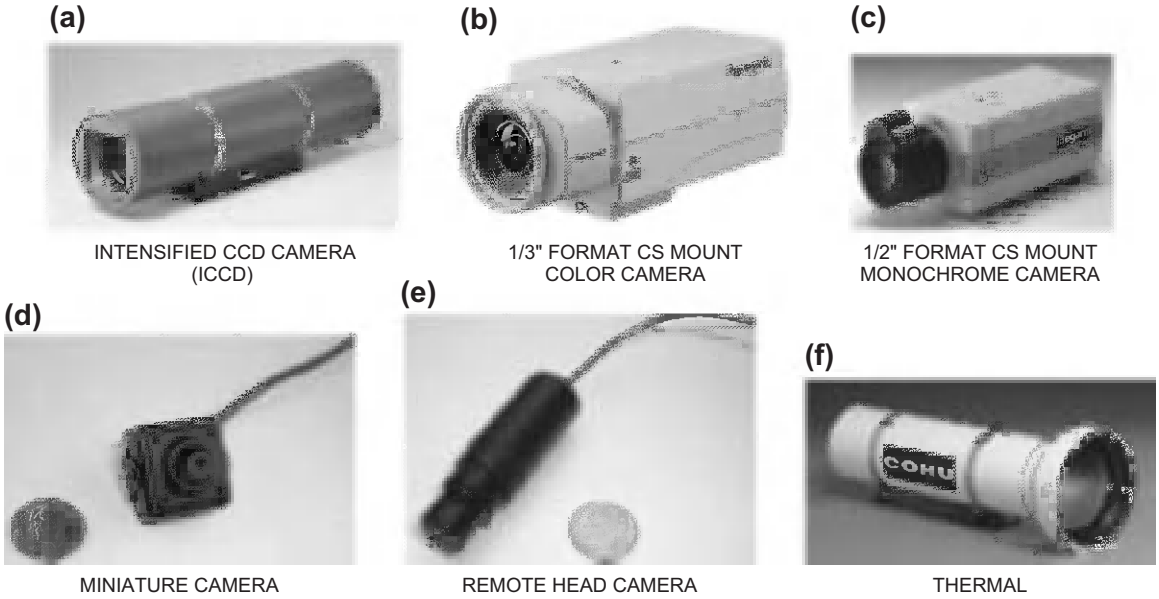


FIGURE 11-10 Representative video cameras.

TABLE 11-1 Light Levels under Daytime and Nighttime Conditions

Condition (fc)	Illumination (lux)	Comments	
Direct sunlight	10,000	107,500	Daylight range
Full daylight	1,000	10,750	
Overcast day	100	1,075	
Very dark day	10	107.5	
Twilight	1	10.75	
Deep twilight	0.1	1.075	
Full moon	0.01	0.1075	LLL range
Quarter moon	0.001	0.01075	
Starlight	0.0001	0.001075	
Overcast night	0.00001	0.0001075	

Note: 1 lux = 0.093 fc.

Natural Light

During daytime the amount of illumination and spectral distribution of light (color) reaching a scene depends on the time of day and atmospheric conditions. The color spectrum of the light reaching the scene is important if color CCTV is used. Direct sunlight produces the highest-contrast scene, allowing maximum identification of objects. On a cloudy or overcast day, less light is received by the objects in the scene resulting in less contrast. To produce an optimum camera picture under the wide variation in light levels (daytime to nighttime), an automatic-iris camera system is required. Table 11-1 shows the light levels for outdoor illumination under bright sun, partial clouds, and overcast day down to overcast night.

Scene illumination is measured in foot-candles (fc) and can vary from 10,000 to 1 (or more). This exceeds the dynamic operating range of most camera sensors for producing a good quality video image.

After the sun has gone below the horizon and if the moon is overhead, reflected sunlight from the

moon illuminates the scene and may be detected by a sensitive monochrome camera. Detection of information in a scene under this condition requires a very sensitive camera, since there is very little light reflected into the camera lens from the scene. As an extreme, when the moon is not overhead or is obscured by cloud cover, the only light received is ambient light from (1) local man-made lighting sources; (2) night-glow caused by distant ground lighting reflecting off particulate (pollution), clouds, and aerosols in the lower atmosphere; and (3) direct light caused by starlight. This is the most severe lighting condition and requires (1) ICCD, (2) monochrome camera with IR light-emitting diode (LED) illumination, or (3) thermal IR camera. Table 11-2 summarizes the light levels occurring under daylight and these LLL conditions and the operating ranges of typical cameras. The equivalent metric measure of light level (lux) compared with the foot-candle (fc) is given. One fc is equivalent to approximately 9.3 lux.

Artificial Light

Artificial illumination is often used to augment outdoor lighting to obtain adequate video surveillance at night. The light sources used are tungsten, tungsten-halogen, metal-arc, mercury, sodium, xenon, IR lamps, and LED IR arrays. Figure 11-11 illustrates several examples of these lamps.

The type of lighting chosen depends on architectural requirements and the specific application. Often a particular lighting design is used for safety reasons so that personnel at the scene can see better and for improving the video picture. Tungsten and tungsten-halogen lamps have by far the most balanced color and are best for color cameras. The most efficient visual outdoor light types are the low- and high-pressure sodium-vapor lamps to which the human eye is most sensitive. These lamps, however, do not produce all colors (missing blue and green) and therefore are not good light sources for color cameras. Metal-arc lamps have excellent color rendition. Mercury-arc lamps provide good security illumination but are missing the color red; therefore, they are not as good as the metal-arc lamps at producing excellent quality color video images. Long-arc xenon lamps with excellent color rendition are often used in outdoor sports arenas and large parking areas.

LED IR illumination arrays mounted in monochrome video cameras or located near

TABLE 11-2 Camera Capability under Natural Lighting Conditions and Camera Requirement per Lighting Conditions

Illumination Condition (fc)	Illumination (lux)	Vidicon*	CCD	CMOS	ICCD	ISIT*
Overcast night	0.00001	0.0001075				
Starlight	0.0001	0.001075				
Quarter moon	0.001	0.01075				
Full moon	0.01	0.1075				
Deep twilight	0.1	1.075				
Twilight	1	10.075				
Very dark day	10	107.5		Operating range of typical cameras		
Overcast day	100	1,075				
Full daylight	1,000	10,750				
Direct sunlight	10,000	107,500				

ISIT = intensified silicon intensified target.
*For reference only.

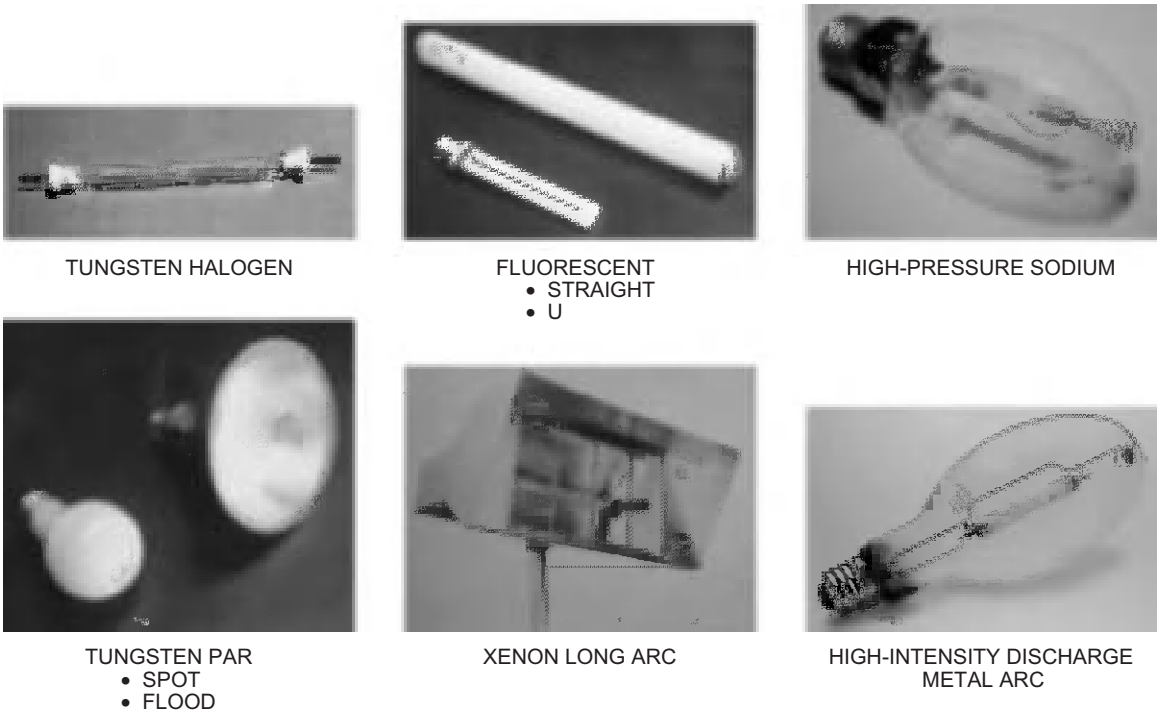


FIGURE 11-11 Representative artificial light sources.

the camera are used to illuminate scenes when there is insufficient lighting. Since they only emit energy in the IR spectrum they can only be used with monochrome cameras. They are used at short ranges (10–25 feet) with wide-angle lenses (50–75° FOV) or at medium long ranges (25–200 feet) with medium to narrow FOV lenses (5–20°).

Artificial indoor illumination is similar to outdoor illumination, with fluorescent lighting used extensively in addition to the high-pressure sodium, metal-arc, and mercury lamps. Since indoor lighting has a relatively constant light level, automatic-iris lenses are often unnecessary. However, if the CCTV camera views a scene near an outside window or a door where additional light comes in during the day, or if the indoor lighting changes between daytime and nighttime operation, then an automatic-iris lens or electronically shuttered camera is required. The illumination level from most indoor lighting is significantly lower by 100–1,000 times than that of sunlight.

SCENE CHARACTERISTICS

The quality of the video image depends on various scene characteristics that include: (1) the scene lighting level; (2) the sharpness and contrast of objects relative to the scene background; (3) whether objects are in a simple, uncluttered background or in a complicated scene; and (4) whether objects are stationary or in motion. These scene factors will determine whether the system will be able to detect, determine orientation, recognize, or identify objects and personnel. As will be seen later, the scene illumination—via sunlight, moonlight, or artificial sources—and the actual scene contrast play important roles in the type of lens and camera necessary to produce a quality image on the monitor.

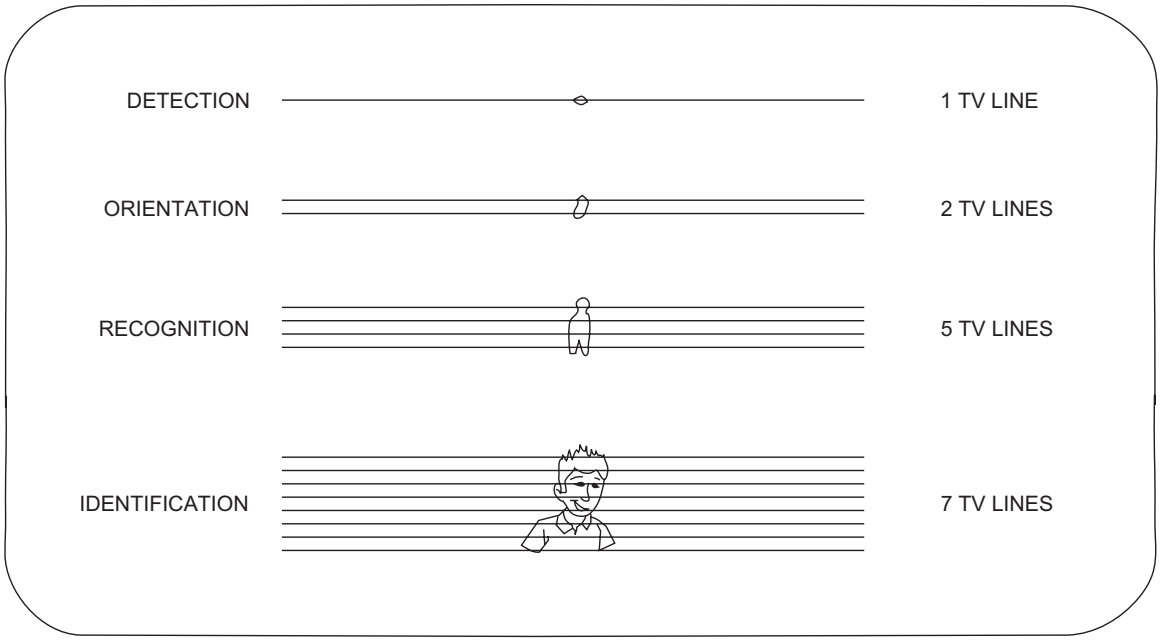


FIGURE 11-12 Object size versus intelligence obtained.

Target Size

In addition to the scene's illumination level and the object's contrast with respect to the scene background, the object's apparent size, that is, its angular FOV as seen by the camera, influences a person's ability to detect it. (Try to find a football referee with a striped shirt in a field of zebras.)

The requirements of a video system are a function of the application. These include: (1) detection of the object or movement in the scene; (2) determination of the object's orientation; (3) recognition of the type of object in the scene, that is, adult or child, car or truck; or (4) identification of the object (Who is the person? Exactly what kind of truck is it?). Making these distinctions depends on the system's resolution, contrast, and signal-to-noise ratio (S/N). In a typical scene the average observer can detect a target about one-tenth of a degree in angle. This can be related to a standard video picture that has 525 horizontal lines (from the National Television System Committee; NTSC) and about 350 TV line vertical and 500 TV line horizontal resolution. Figure 11-12 and Table 11-3 summarize the number of lines required to detect, orient, recognize, or identify an object in a television picture. The number of TV lines required will increase for conditions of poor lighting, highly complex backgrounds, reduced contrast, or fast movement of the camera or target.

TABLE 11-3 TV Lines versus Intelligence Obtained

Intelligence	Minimum TV Lines*
Detection	1 ± 0.25
Orientation	1.4 ± 0.35
Recognition	4 ± 0.8
Identification	6.4 ± 1.5

*One TV line corresponds to a light and dark line (one TV line pair).

Reflectivity

The reflectivity of different materials varies greatly depending on its composition and surface texture. Table 11-4 gives some examples of materials and objects viewed by video cameras and their respective reflectivity.

TABLE 11-4 Reflectivity of Common Materials

Material	Reflectivity (%)*
Snow	85–95
Asphalt	5
Plaster (white)	90
Sand	40–60
Trees	20
Grass	40
Clothes	15–30
Concrete—new	40
Concrete—old	25
Clear windows	70
Human face	15–25
Wood	10–20
Painted wall (white)	75–90
Red brick	25–35
Parking lot and automobiles	40
Aluminum building (diffuse)	65–70

*Visible spectrum: 400–700 nm.

Since the camera responds to the amount of light reflected from the scene, it is important to recognize that objects have a large range of reflectivity. The objects with the highest reflectivity produce the brightest images. To detect one object located within the area of another the objects must differ in reflectivity, color, or texture. Therefore, if a red box is in front of a green wall and both have the same reflectivity and texture, the box will not be seen on a monochrome video system. In this case, the total reflectivity in the visible spectrum is the same for the green wall and the red box. This is where the color camera shows its advantage over the monochrome camera.

The case of a color scene is more complex. While the reflectivity of the red box and the green wall may be the same as averaged over the entire visible spectrum from blue to red, the color camera can distinguish between green and red.

It is easier to identify a scene characteristic by a difference in color in a color scene than it is to identify it by a difference in gray scale (intensity) in a monochrome scene. For this reason the target size required to make an identification in a color scene is generally less than it is to make the same identification in a monochrome scene.

Effects of Motion

A moving object in a video image is easier to detect but more difficult to recognize than a stationary one provided that the camera can respond to it. LLL cameras produce sharp images for stationary scenes but smeared images for moving targets. This is caused by a phenomenon called "lag" or "smear." Solid-state sensors (CCD, CMOS, and ICCD) do not exhibit smear or lag at normal light levels; therefore, they can produce sharp images of both stationary and moving scenes. Some image intensifiers exhibit smear when the scene moves fast or when there is a bright light in the FOV of the lens.

When the target in the scene moves very fast the inherent camera scan rate (30 frames per second, fps) causes a blurred image of this moving target in the camera. This is analogous to the blurred image in a still photograph when the shutter speed is too slow for the action. There is no cure for this as long as the standard NTSC television scan rate (30 fps) is used. However, CCTV snapshots can be taken without any blurring using fast-shuttered CCD cameras. For special applications in which fast-moving targets must be imaged and tracked, higher scan rate cameras are available.

Scene Temperature

Scene temperature has no effect on the video image in a CCD, CMOS, or ICCD sensor. These sensors do not respond to temperature changes or temperature differences in the scene. On the other hand, IR thermal imaging cameras do respond to temperature differences and changes in temperature in the scene. Thermal imagers do not respond to visible light or the very near-IR radiation like that produced by IR LEDs. The sensitivity of IR thermal imagers is defined as the smallest change in temperature in the scene that can be detected by the thermal camera.

LENSES

A lens collects reflected light from the scene and focuses it onto the camera image sensor. This is analogous to the lens of the human eye focusing a scene onto the retina at the back of the eye (Figure 11-6). As in the human eye, the camera lens inverts the scene image on the image sensor, but the eye and the camera electronics compensate (invert the image) to perceive an upright scene. The retina of the human eye differs from any CCTV lens in that it focuses a sharp image only in the central 10% of its total 160° FOV. All vision outside the central focused scene is out of focus. This central imaging part of the human eye can be characterized as a medium FL lens that is 16–25 mm. In principle, Figure 11-6 represents the function of any lens in a video system.

Many different lens types are used for video surveillance and safety applications. They range from the simplest FFL manual-iris lenses to the more complex varifocal and zoom lenses, with an automatic iris being an option for all types.

In addition, pinhole lenses are available for covert applications, split-image lenses for viewing multiple scenes on one camera, right-angle lenses for viewing a scene perpendicular to the camera axis, and rigid or flexible fiber optic lenses for viewing through thick walls, under doors, and so forth.

FFL Lens

Figure 11-13 illustrates three fixed FFL or fixed FOV lenses with narrow (telephoto), medium, and wide FOVs and the corresponding FOV obtained when used with a 1/3-inch camera sensor format.

Wide FOV (short FL) lenses permit viewing a very large scene (wide angle) with low

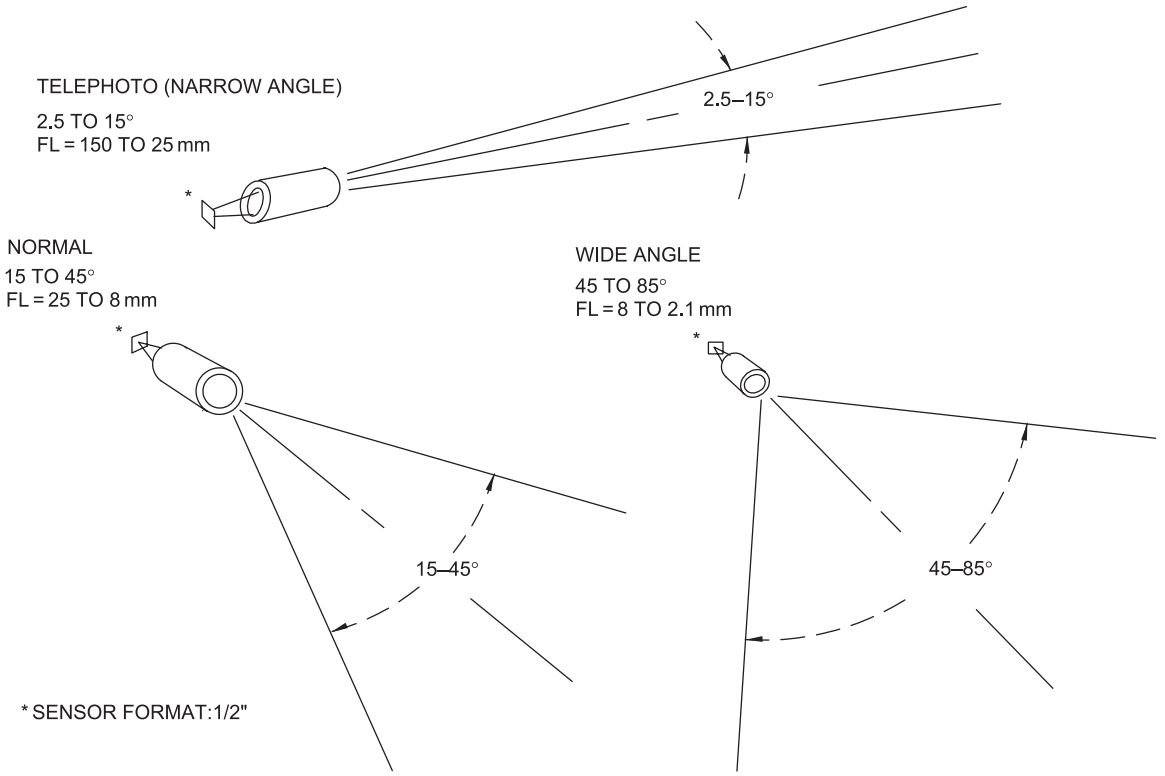


FIGURE 11-13 Representative FFL lenses and their FOVs.

magnification and therefore provide low resolution and low identification capabilities. Narrow FOV or telephoto lenses have high magnification with high resolution and high identification capabilities.

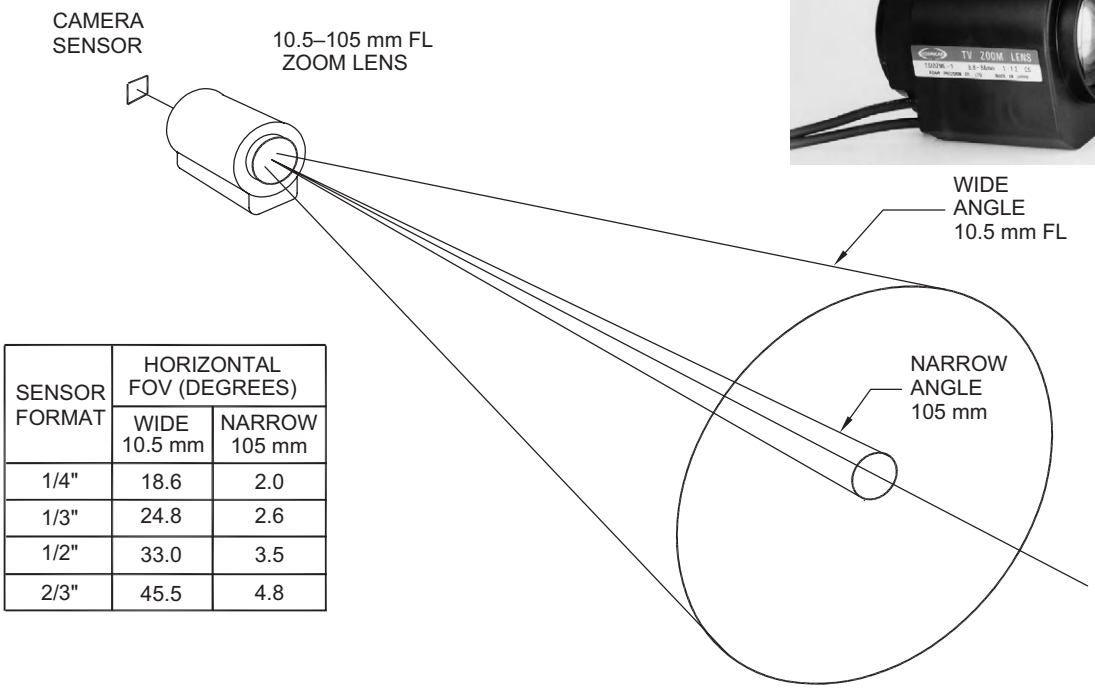
Zoom Lens

The zoom lens is more versatile and complex than the FFL lens. Its FL is variable from wide-angle to narrow-angle (telephoto) FOV (Figure 11-14).

The overall camera/lens FOV depends on the lens FL and the camera sensor size as shown in Figure 11-14. Zoom lenses consist of multiple lens groups that are moved within the lens barrel by means of an external zooming ring (manual or motorized), changing the lens FL and angular FOV without having to switch lenses or refocusing. Zoom focal length ratios can range from 6:1 up to 50:1. Zoom lenses are usually large and used on pan/tilt mounts viewing over large areas and distances (25–500 feet).

Varifocal Lens

The varifocal lens is a variable focal length lens used in applications where an FFL lens would be used. In general they are smaller and cost much less than zoom lenses. Like the zoom lens, the varifocal lens is used because its focal length (angular FOV) can be changed manually or automatically, using a motor, by rotating the barrel on the lens. This feature makes it convenient to adjust the FOV to a precise angle when installed on the camera. Typical varifocal lenses have focal lengths of 3–8 mm, 5–12 mm, and 8–50 mm. With just these three lenses focal lengths from 3 mm to 50 mm (91–5° horizontal FOV) can be covered on a $^1/_3$-inch format sensor. Unlike zoom lenses, varifocal lenses must be refocused each time the FL and the FOV are



SENSOR FORMAT	HORIZONTAL FOV (DEGREES)	
	WIDE 10.5 mm	NARROW 105 mm
1/4"	18.6	2.0
1/3"	24.8	2.6
1/2"	33.0	3.5
2/3"	45.5	4.8

FIGURE 11-14 Zoom video lens horizontal FOV.

changed. They are not suitable for zoom or pan/tilt applications.

Panoramic 360° Lens

There has always been a need to see "all around," that is, an entire room or other location, seeing 360° with *one* panoramic camera and lens. In the past, 360° FOV camera viewing systems have only been achieved by using multiple cameras and lenses and combining the scenes on a split-screen monitor.

Panoramic lenses have been available for many years but have only recently been combined with digital electronics and sophisticated mathematical transformations to take advantage of their capabilities. Figure 11-15 shows two lenses having a 360° horizontal FOV and a 90° vertical FOV.

The panoramic lens collects light from the 360° panoramic scene and focuses it onto the camera sensor as a donut-shaped image. The electronics and mathematical algorithm convert this donut-shaped panoramic image into the rectangular (horizontal and vertical) format for normal monitor viewing.

Covert Pinhole Lens

This special security lens is used when the lens and CCTV camera must be hidden. The front lens element or aperture is small (from $^1/_{16}$ to $^5/_{16}$ of an inch in diameter). Although this is not the size of a pinhead, it nevertheless has been labeled as such. Figure 11-16 shows examples of straight and right-angle pinhole lenses used with C or CS mount cameras. The very small mini-pinhole lenses are used on the low-cost, small board cameras.

Special Lenses

Some special lenses useful in security applications include split-image, right-angle, relay, and fiber optic (Figure 11-17).

The dual-split and tri-split lenses use only one camera to produce multiple scenes. These are useful for viewing the same scene with different magnifications or different scenes with the same or different magnifications. Using only one camera can reduce cost and increase reliability. These lenses are useful when two or three views are required and only one camera was installed.

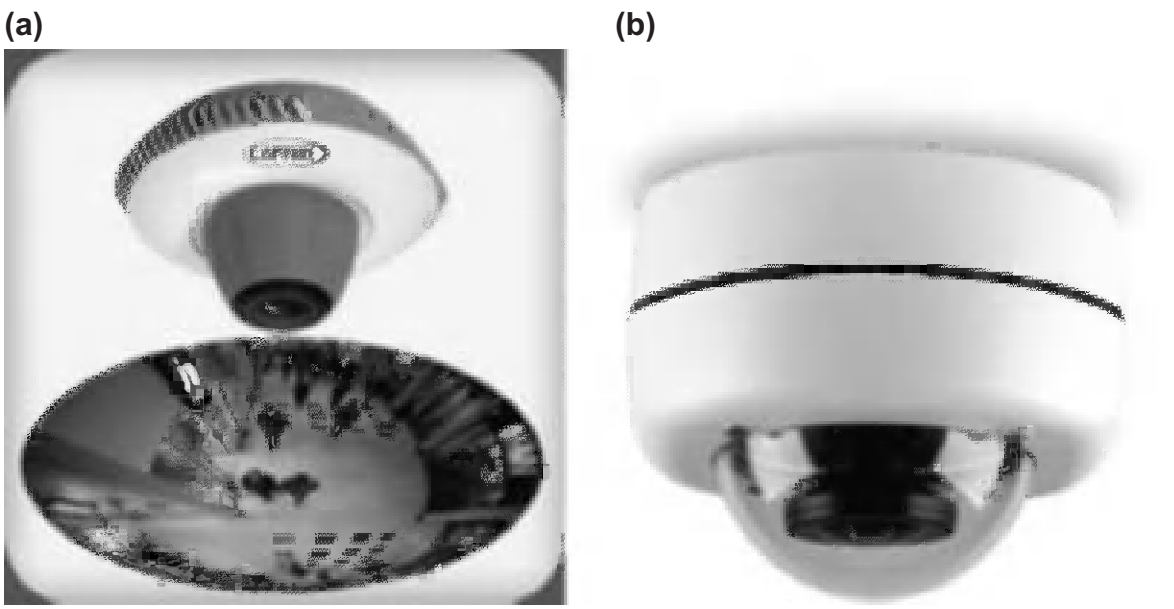


FIGURE 11-15 Panoramic 360° lens.

(a)

PINHOLE LENSES

(b)

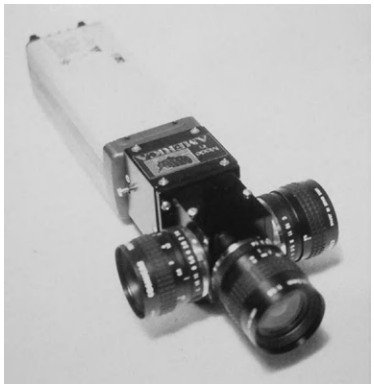
MINI-LENSES

FIGURE 11-16 Pinhole and mini-pinhole lenses.

(a)

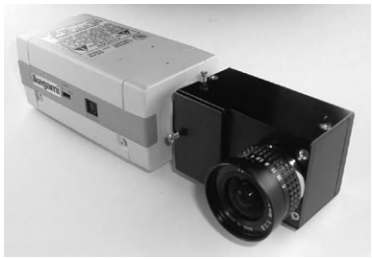
DUAL SPLIT IMAGE LENS

(b)



TRI SPLIT IMAGE LENS

(c)



RIGHT ANGLE LENS

(d)

RIGID FIBER OPTICS

(e)

RELAY LENS

(f)

FLEXIBLE FIBER OPTICS

FIGURE 11-17 Special video lenses.

The right-angle lens permits a camera using a wide-angle lens installed to view a scene that is perpendicular to the camera's optical axis. There are no restrictions on the focal lengths so they can be used in wide- or narrow-angle applications.

The flexible and rigid coherent fiber optic lenses are used to mount a camera several inches to several feet away from the front lens as might be required to view from the opposite side of a wall or in a hazardous environment. The function of the fiber optic bundle is to transfer the focused visual image from one location to another. This may be useful for (1) protecting the camera and (2) locating the lens in one environment (outdoors) and the camera in another (indoors).

CAMERAS

The camera lens focuses the visual scene image onto the camera sensor area point by point and the camera electronics transforms the visible image into an electrical signal. The camera video signal (containing all picture information) is made up of frequencies from 30 cycles per second, or 30 Hz, to 4.2 million cycles per second, or 4.2 MHz. The video signal is transmitted via a cable (or wireless) to the monitor display.

Almost all security cameras in use today are color or monochrome CCD with the rapid emergence of CMOS types. These cameras are available as low-cost single printed circuit board (PCB) cameras with small lenses already built in, with or without a housing used for covert and overt surveillance applications. More expensive cameras in a housing are larger and more rugged and have a C or CS mechanical mount for accepting any type of lens. These cameras have higher resolution and light sensitivity and other electrical input/output features suitable for multiple camera CCTV systems. The CCD and CMOS cameras with LED IR illumination arrays can extend the use of these cameras to nighttime use. For LLL applications, the ICCD and IR cameras provide the highest sensitivity and detection capability.

Significant advancements in camera technology have been made in the last few years, particularly in the use of DSP in the camera and development of the IP camera. All security cameras manufactured between the 1950s and 1980s were the vacuum tube type, either vidicon, silicon, or LLL types using silicon intensified target (SIT) and ISIT. In the 1980s the CCD and CMOS solid-state video image sensors were developed and remain the mainstay in the security industry. Increased consumer demand for video recorders using CCD sensors in camcorders and the CMOS sensor in digital still frame cameras caused a technology explosion and made these small, high-resolution, high-sensitivity, monochrome and color solid-state cameras available for security systems.

The security industry now has both analog and digital surveillance cameras at its disposal. Up until the mid-1990s analog cameras dominated, with only rare use of DSP electronics, and the digital Internet camera was only being introduced to the security market. Advances in solid-state circuitry, the demand from the consumer market, and the availability of the Internet were responsible for the rapid use of digital cameras for security applications.

The Scanning Process

Two methods used in the camera and monitor video scanning process are *raster* scanning and *progressive* scanning. In the past, analog video systems have all used the raster scanning technique; however, newer digital systems are now using progressive scanning. All cameras use some form of scanning to generate the video picture. A block diagram of the CCTV camera and a brief description of the analog raster scanning process and video signal are shown in Figures 11-8, 11-9, 11-18, and 11-19.

The camera sensor converts the optical image from the lens into an electrical signal. The camera electronics process the video signal and generate a composite video signal containing the picture information (luminance and color) and horizontal and vertical synchronizing pulses.

Signals are transmitted in what is called a *frame* of picture video, made up of two *fields* of information. Each field is transmitted in $^1/_{60}$ of a

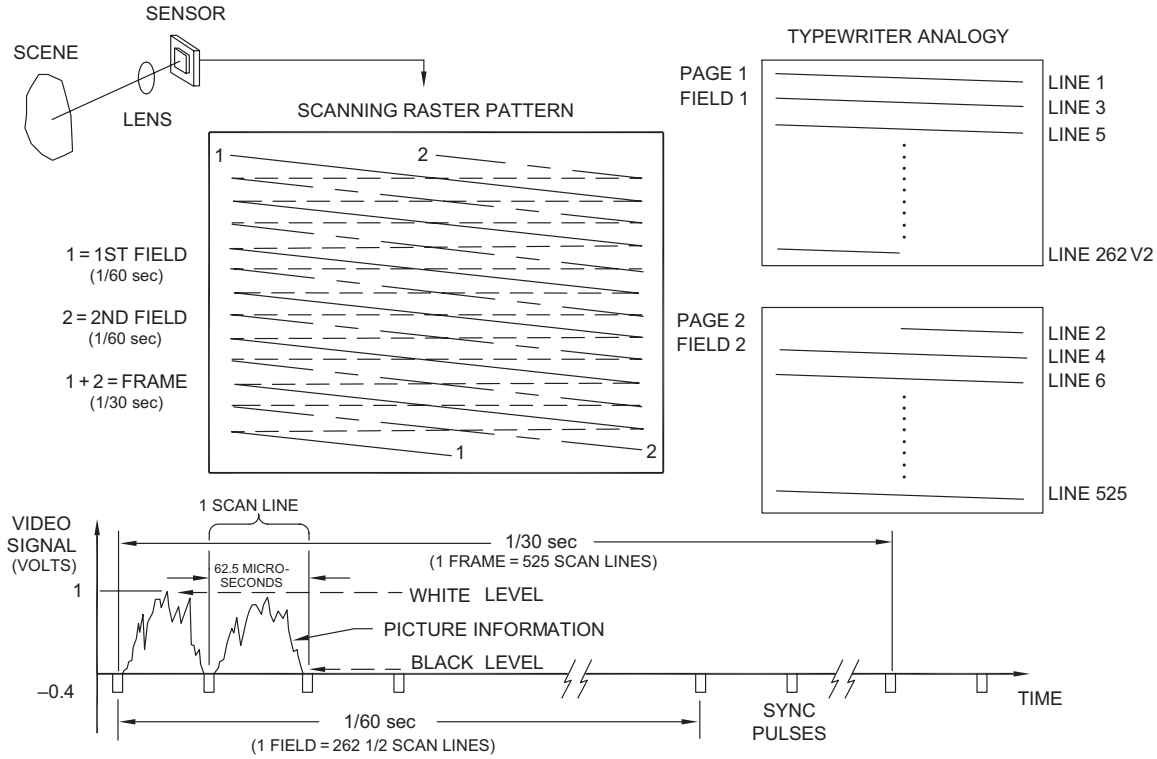


FIGURE 11-18 Analog video scanning process and video display signal.

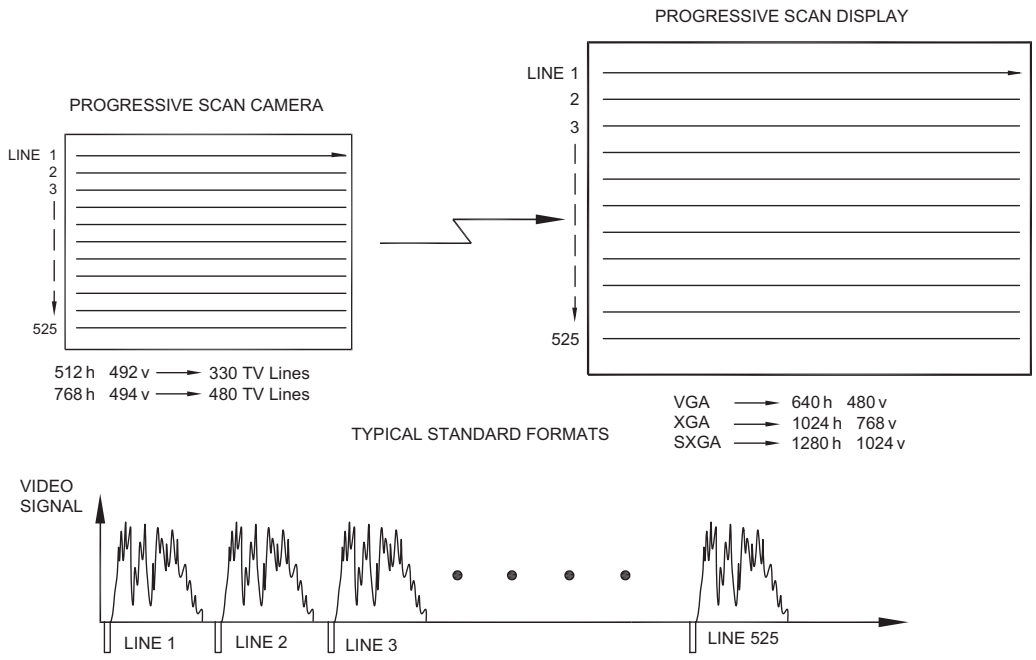


FIGURE 11-19 Digital and progressive scanning process and video display signal.

second and the entire frame in $^1/_{30}$ of a second, for a repetition rate of 30 fps. In the United States, this format is the Electronic Industries Association (EIA) standard called the NTSC system. The European standard uses 625 horizontal lines with a field taking $^1/_{50}$ of a second and a frame $^1/_{25}$ of a second and a repetition rate of 25 fps.

Raster Scanning. In the NTSC system the first picture field is created by scanning 262½ horizontal lines. The second field of the frame contains the second 262½ lines, which are synchronized so that they fall between the gaps of the first field lines thus producing one completely interlaced picture frame containing 525 lines. The scan lines of the second field fall *exactly* halfway between the lines of the first field resulting in a 2-to-1 *interlace* system. As shown in Figure 11-18 the first field starts at the upper left corner (of the camera sensor or the CRT monitor) and progresses down the sensor (or screen), line by line, until it ends at the bottom center of the scan.

Likewise the second field starts at the top center of the screen and ends at the lower-right corner. Each time one line in the field traverses from the left side of the scan to the right it corresponds to one horizontal line as shown in the video waveform at the bottom of Figure 11-18. The video waveform consists of negative synchronization pulses and positive picture information. The horizontal and vertical synchronization pulses are used by the video monitor (and VCR, DVR, or video printer) to synchronize the video picture and paint an exact replica in time and intensity of the camera scanning function onto the monitor face. Black picture information is indicated on the waveform at the bottom (approximately 0 V) and the white picture information at the top (1 V). The amplitude of a standard NTSC signal is 1.4 V peak to peak. In the 525-line system the *picture* information consists of approximately 512 lines. The lines with no picture information are necessary for vertical blanking, which is the time when the camera electronics or the beam in the monitor CRT moves from the bottom to the top to start a new field.

Random-interlace cameras do not provide complete synchronization between the first and the second fields. The horizontal and the vertical scan frequencies are not locked together, therefore, fields do not interlace exactly. This condition, however, results in an acceptable picture, and the asynchronous condition is difficult to detect. The 2-to-1 interlace system has an advantage when multiple cameras are used with multiple monitors and/or recorders in that they prevent jump or jitter when switching from one camera to the next.

The scanning process for solid-state cameras is different. The solid-state sensor consists of an array of very small picture elements (pixels) that are read out serially (sequentially) by the camera electronics to produce the same NTSC format—525 TV lines in 1/30 of a second (30 fps)—as shown in Figure 11-19.

The use of digital cameras and digital monitors has changed the way the camera and monitor signals are processed, transmitted, and displayed. The final presentation on the monitor looks similar to the analog method, but instead of seeing 525 horizontal lines (NTSC system) individual pixels are seen in a *row* and *column* format. In the digital system the camera scene is divided into rows and columns of individual pixels (small points in the scene) each representing the light intensity and color for each point in the scene. The digitized scene signal is transmitted to the digital display, be it LCD, plasma, or other, and reproduced on the monitor screen pixel by pixel, providing a faithful representation of the original scene.

Digital and Progressive Scan. The digital scanning is accomplished in the 2-to-1 interlace mode as in the analog system, or in a *progressive* mode. In the progressive mode each line is scanned in linear sequence: line 1, then line 2, line 3, and so forth. Solid-state camera sensors and monitor displays can be manufactured with a variety of horizontal and vertical pixels formats. The standard aspect ratio is 4:3 as in the analog system, and 16:9 for the wide screen. Likewise there are many different combinations of pixel numbers available in the sensor and display. Some standard formats for color CCD cameras are 512 h × 492 v for 330 TV line resolution and 768 h × 494 v for 480 TV

line resolution, and for color LCD monitors it is 1280 h × 1024 v.

Solid-State Cameras

Video security cameras have gone through rapid technological change during the last half of the 1980s to the present. For decades the vidicon tube camera was the only security camera available. In the 1980s the more sensitive and rugged silicon-diode tube camera was the best available. In the late 1980s the invention and development of the digital CCD and later the CMOS cameras replaced the tube camera. This technology coincided with rapid advancement in DSP in cameras, the IP camera, and use of digital transmission of the video signal over LAN, WANs, and the Internet. The two generic solid-state cameras that account for most security applications are the CCD and the CMOS.

The first generation of solid-state cameras available from most manufacturers had $^2/_3$-inch (sensor diagonal) and ½-inch sensor formats. As the technology improved, smaller formats evolved. Most solid-state cameras in use today are available in three image sensor formats: ½ inch, $^1/_3$ inch, and $^1/_4$ inch. The ½-inch format produces higher resolution and sensitivity at a higher cost. The ½-inch and smaller formats permitted the use of smaller, less expensive lenses as compared with the larger formats. Many manufacturers now produce $^1/_3$-inch and ¼-inch format cameras with excellent resolution and light sensitivity. Solid-state sensor cameras are superior to their predecessors because of their (1) precise, repeatable pixel geometry, (2) low power requirements, (3) small size, (4) excellent color rendition and stability, and (5) ruggedness and long life expectancy. At present, solid-state cameras have settled into three main categories: (1) analog, (2) digital, and (3) Internet.

Analog. Analog cameras have been with the industry since CCTV has been used in security. Their electronics are straightforward and the technology is still used in many applications.

Digital. Since the second half of the 1990s there has been an increased use of DSP in cameras. It significantly improves the performance of the camera by (1) automatically adjusting to large light level changes (eliminating the automatic-iris), (2) integrating the VMD into the camera, and (3) automatically switching the camera from color operation to higher sensitivity monochrome operation, as well as other features and enhancements.

Internet. The most recent camera technology advancement is manifest in the IP camera. This camera is configured with electronics that connects to the Internet and the WWW network through an Internet service provider (ISP). Each camera is provided with a registered Internet address and can transmit the video image anywhere on the network. This is really remote video monitoring at its best. The camera site is viewed from anywhere by entering the camera Internet address (ID number) and proper password. Password security is used so that only authorized users can enter the Web site and view the camera image. Two-way communication is used so that the user can control camera parameters and direct the camera operation (pan, tilt, zoom, etc.) from the monitoring site.

LLL-Intensified Camera

When a security application requires viewing during nighttime conditions where the available light is moonlight, starlight, or other residual reflected light, and the surveillance must be covert (no active illumination like IR LEDs), LLL-intensified CCD cameras are used. The ICCD cameras have sensitivities between 100 and 1,000 times higher than the best solid-state cameras. The increased sensitivity is obtained through the use of a *light amplifier* mounted in between the lens and the CCD sensor. LLL cameras cost between 10 and 20 times more than CCD cameras.

Thermal Imaging Camera

An alternative to the ICCD camera is the thermal IR camera. Visual cameras see only visible light energy from the blue end of the visible spectrum to the red end (approximately 400–700 nm). Some monochrome cameras see beyond the

visible region into the near-IR region of the spectrum up to 1,000 nm. This IR energy, however, is not thermal IR energy. Thermal IR cameras using thermal sensors respond to thermal energy in the 3–5 and 8–14 μm range. The IR sensors respond to the changes in *heat* (thermal) energy emitted by the targets in the scene. Thermal imaging cameras can operate in complete darkness as they require no visible or IR illumination whatever. They are truly passive nighttime monochrome imaging sensors. They can detect humans and any other warm objects (animals, vehicle engines, ships, aircraft, warm/hot spots in buildings) or other objects against a scene background.

Panoramic 360° Camera

Powerful mathematical techniques combined with the unique 360° panoramic lens have made a 360° panoramic camera possible. In operation the lens collects and focuses the 360° horizontal by up to 90° vertical scene (one-half of a sphere; a hemisphere) onto the camera sensor. The image takes the form of a "donut" on the sensor (Figure 11-20).

The camera/lens is located at the origin (0). The scene is represented by the surface of the hemisphere. As shown, a small part (slice) of the scene area (A, B, C, D) is "mapped" onto the sensor as a, b, c, d. In this way the full scene is mapped onto the sensor. Direct presentation of the donut-ring video image onto the monitor does not result in a useful picture.

That is where the use of a powerful mathematical algorithm comes in. Digital processing in the computer using the algorithm transforms the donut-shaped image into the normal format seen on a monitor, that is, horizontal and vertical.

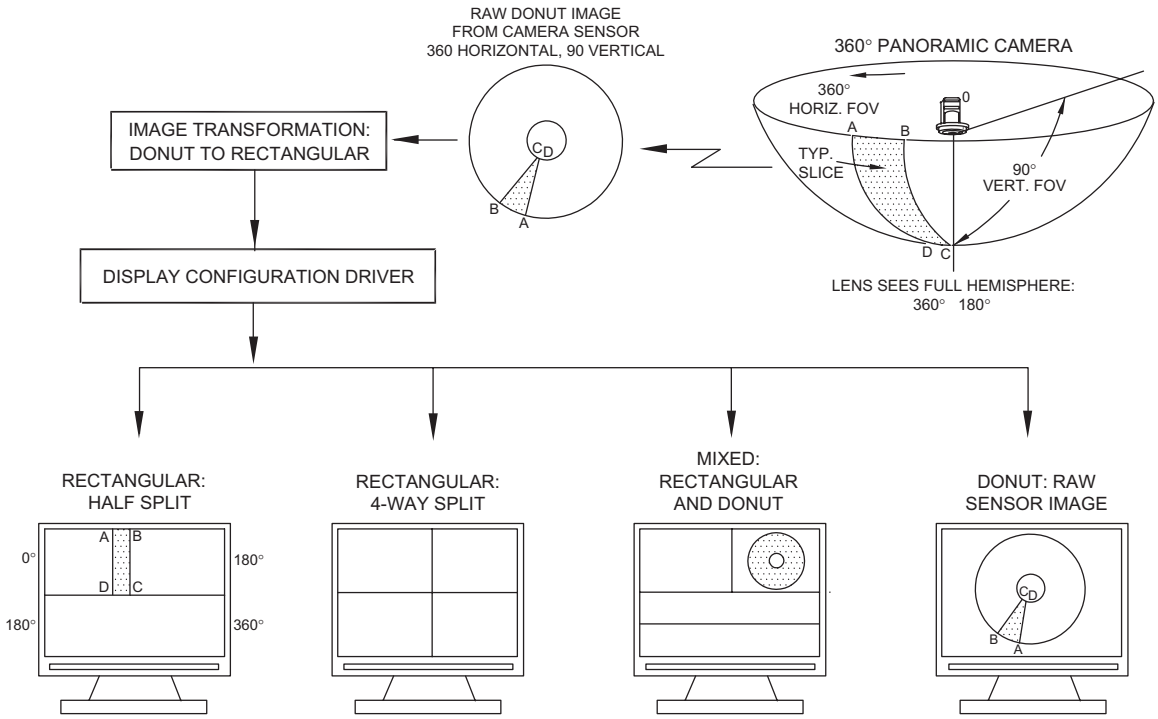


FIGURE 11-20 Panoramic 360° camera.

All of the 0–360° horizontal by 90° vertical images cannot be presented on a monitor in a useful way—there is just too much picture "squeezed" into the small screen area. This condition is solved by computer software by looking at only a section of the entire scene at any particular time.

The main attributes of the panoramic system include: (1) capturing a full 360° FOV, (2) the ability to digitally pan/tilt to anywhere in the scene and digitally zoom any scene area, (3) having no moving parts (no motors, etc., that can wear out), and (4) having multiple operators that can view any part of the scene in real time or at a later time.

The panoramic camera requires a high-resolution camera since so much scene information is contained in the image. Camera technology has progressed so that these digital cameras are available and can present a good image of a zoomed-in portion of the panoramic scene.

TRANSMISSION

By definition, the camera must be remotely located from the monitor and therefore the video signal must be transmitted by some means from one location to another. In security applications, the distance between the camera and the monitor may be from tens of feet to many miles or, perhaps, completely around the globe. The transmission path may be inside buildings, outside buildings, above ground, underground, through the atmosphere, or in almost any environment imaginable. For this reason the transmission means must be carefully assessed and an optimum choice of hardware made to satisfactorily transmit the video signal from the camera to the monitoring site. There are many ways to transmit the video signal from the camera to the monitoring site. Figure 11-21 shows some examples of transmission cables.

The signal can be analog or digital. It can be transmitted via electrical conductors using

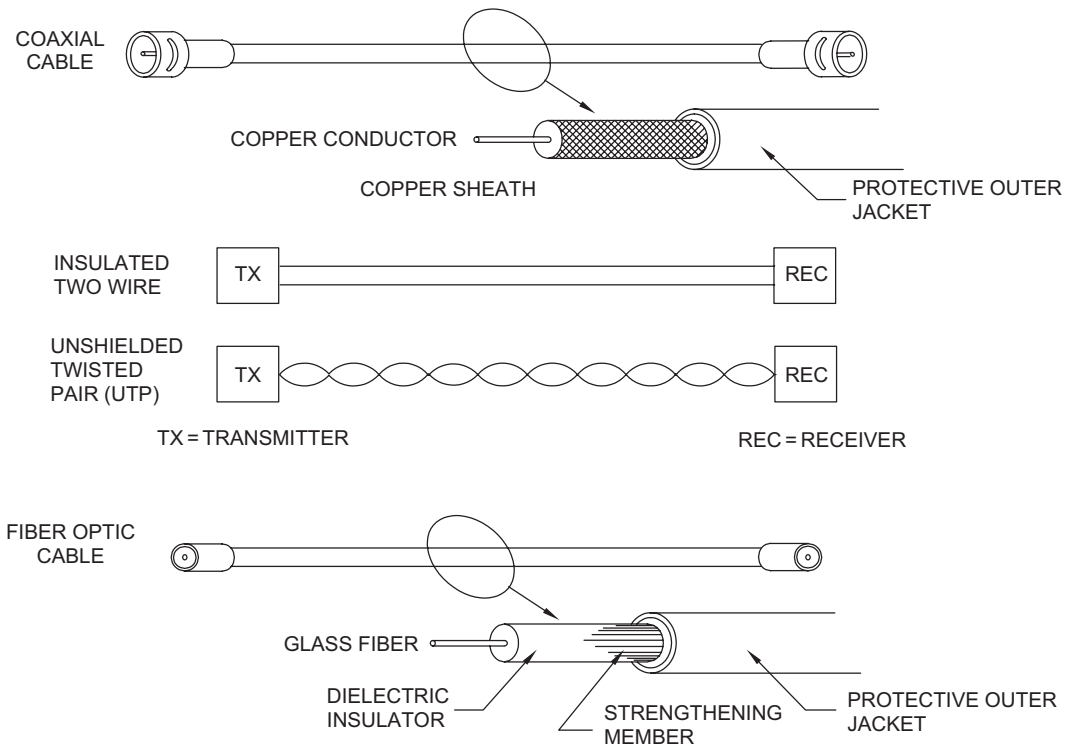


FIGURE 11-21 Hard-wired copper and fiber optic transmission means.

coaxial cable or UTP, by fiber optic, by LAN or WAN, and intranet or Internet.

Particular attention should be paid to transmission means when transmitting color video signals, since the color signal is significantly more complex and susceptible to distortion than monochrome. There are advantages and disadvantages of all of the transmission means and the hardware available to transmit the video signal.

Hard-Wired

There are several hard-wired means for transmitting a video signal: coaxial cable, UTP, LAN, WAN, intranet, Internet, and fiber optic cable.

Fiber optic cable is used for long distances and when there is interfering electrical noise. LANs and Internet connections are digital transmission techniques used in larger security systems and where the signal must be transmitted over existing computer networks or over long distances.

Coaxial Cable. The most common video signal transmission method is the coaxial cable. This cable has been used since the inception of CCTV and is still in use today. The cable is inexpensive and easy to terminate at the camera and monitor ends, and it transmits a faithful video signal with little or no distortion or loss. It has a 75-ohm electrical impedance, which matches the impedance of the camera and monitor, ensuring a distortion-free video image. This coaxial cable has a copper electrical shield and center conductor that works well over distances up to 1,000 feet.

UTP. In the 1990s UTP video transmission came into vogue. The technique uses a transmitter at the camera and a receiver at the monitor with two twisted copper wires connecting them. Several reasons for its increased popularity are that (1) it can be used over longer distances than coaxial cable, (2) it uses inexpensive wire, (3) many locations already have two-wire twisted-pair installed, (4) it uses a low-cost transmitter and receiver, and (5) it has higher electrical noise immunity as compared to coaxial cable. The UTP using a sophisticated electronic transmitter and receiver can transmit the video signal 2,000–3,000 feet.

LAN, WAN, Intranet, and Internet. The evolution of the LAN, WAN, intranet, and Internet revolutionized the transmission of video signals in a new form (digital) which significantly expanded the scope and effectiveness of video for security systems. The widespread use of business computers and consequent use of these networks provided an existing digital network protocol and communications suitable for video transmission. The Internet and WWW attained widespread use in the late 1990s and truly revolutionized digital video transmission. This global computer network provided the digital backbone path to transmit digital video, audio, and command signals from anywhere on the globe.

The video signal transmission techniques described so far provide a means for real-time transmission of a video signal, requiring a full 4.2-MHz bandwidth to reproduce real-time motion. When these techniques cannot be used for real-time video, alternative digital techniques are used. In these systems, a non-real-time video transmission takes place, so that some scene action is lost. Depending on the action in the scene, the resolution, from near real time (15 fps) to slow scan (a few fps) of the video image is transmitted. The digitized and compressed video signal is transmitted over a LAN or Internet network and decompressed and reconstructed at the receiver/monitoring site.

Wireless

In legacy analog video surveillance systems, it is often more economical or beneficial to transmit the real-time video signal without cable (wireless) from the camera to the monitor using an RF or IR atmospheric link. In digital video systems using digital transmission, the use of wireless networks (WiFi) permits routing the video and control signals to *any* remote location. In both the analog and the digital systems some form of video scrambling or encryption is often used to remove the possibility of eavesdropping by unauthorized personnel outside the system. Three

important applications for wireless transmission include: (1) covert and portable rapid deployment video installations, (2) building-to-building transmission over a roadway, and (3) parking lot light poles to building. The Federal Communications Commission (FCC) restricts some wireless transmitting devices using microwave frequencies or RF to government and law enforcement use but has given approval for many RF and microwave transmitters for general security use. These FCC-approved devices operate above the normal television frequency bands at approximately 920 MHz and 2.4 and 5.8 GHz. The atmospheric IR link is used when a high-security link is required. This link does not require an FCC approval and transmits a video image over a narrow beam of visible light or near-IR energy. The beam is very difficult to intercept (tap). Figure 11-22 illustrates some of the wireless transmission techniques available today.

Fiber Optics

Fiber optic transmission technology has advanced significantly in the last 5–10 years and represents a highly reliable, secure means of transmission. Fiber optic transmission holds several significant advantages over other hard-wired systems: (1) very long transmission paths up to many miles without any significant degradation in the video signal with monochrome or color; (2) immunity to external electrical disturbances from weather or electrical equipment; (3) very wide bandwidth, permitting one or more video, control, and audio signals to be multiplexed on a single fiber; and (4) resistance to tapping (eavesdropping) and therefore a very secure transmission means.

While the installation and termination of fiber optic cable requires a more skilled technician, it is well within the capability of qualified security installers. Many hard-wired installations

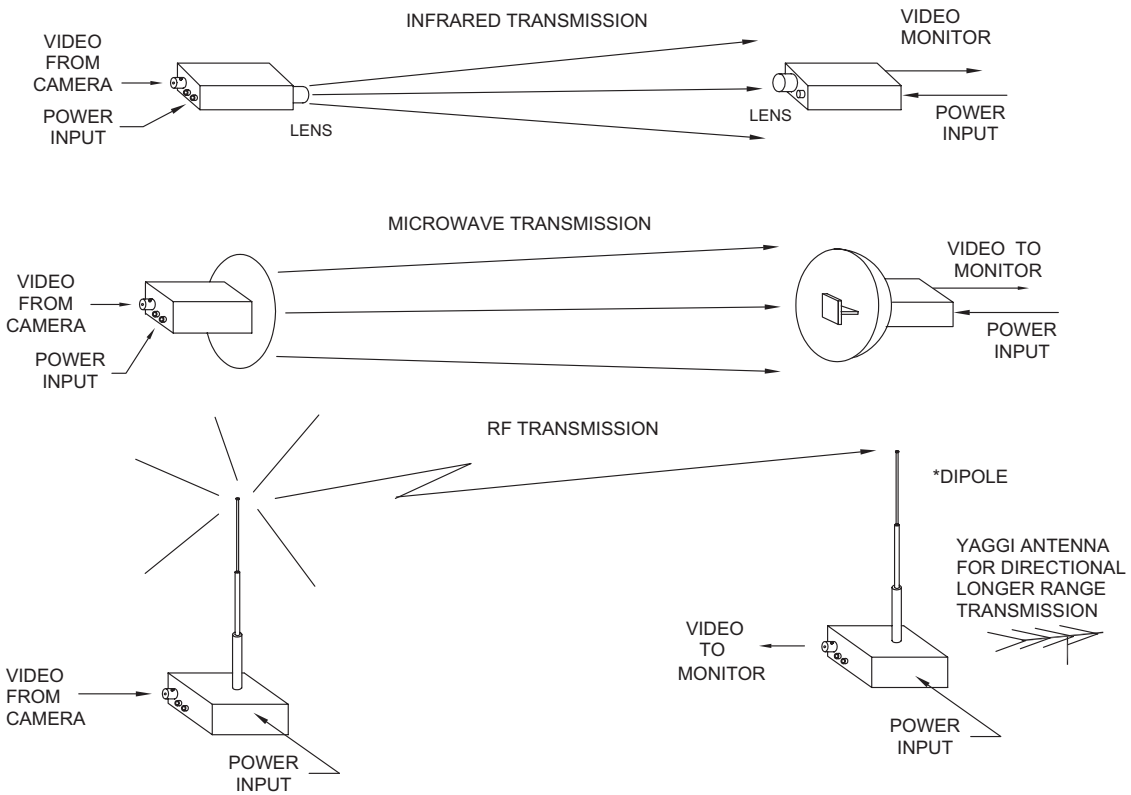


FIGURE 11-22 RF, microwave, and IR video transmission links.

requiring the optimum color and resolution rendition use fiber optic cable.

SWITCHERS

The video switcher accepts video signals from many different video cameras and connects them to one or more monitors or recorders. Using manual or automatic activation or an alarming signal input, the switcher selects one or more of the cameras and directs its video signal to a specified monitor, recorder, or some other device or location.

Standard

There are four basic switcher types: manual, sequential, homing, and alarming. Figure 11-23 shows how these are connected into the video security system.

The manual switcher connects one camera at a time to the monitor, recorder, or printer. The sequential switcher automatically switches the cameras in sequence to the output device. The operator can override the automatic sequence with the homing sequential switcher. The alarming switcher connects the alarmed camera to the output device automatically, when an alarm is received.

Microprocessor Controlled

When the security system requires many cameras in various locations with multiple monitors and other alarm input functions, a microprocessor-controlled

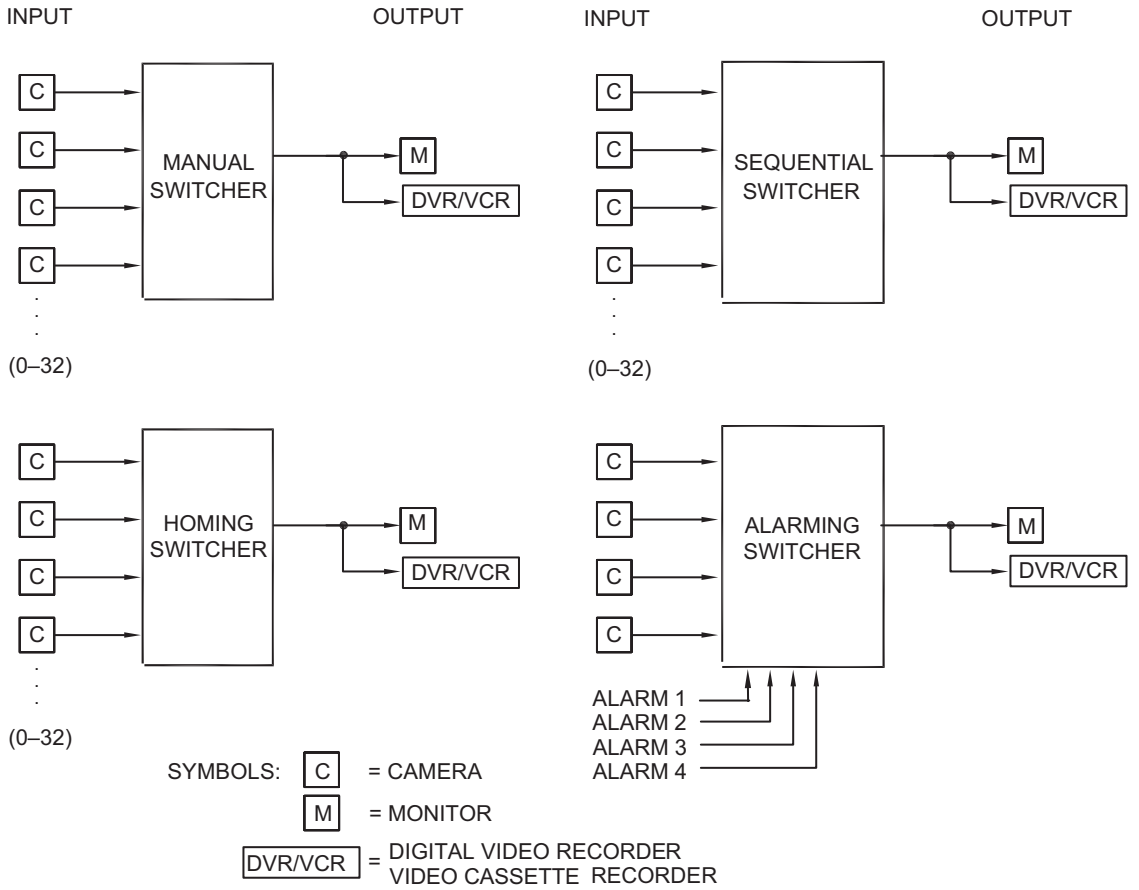


FIGURE 11-23 Basic video switcher types.

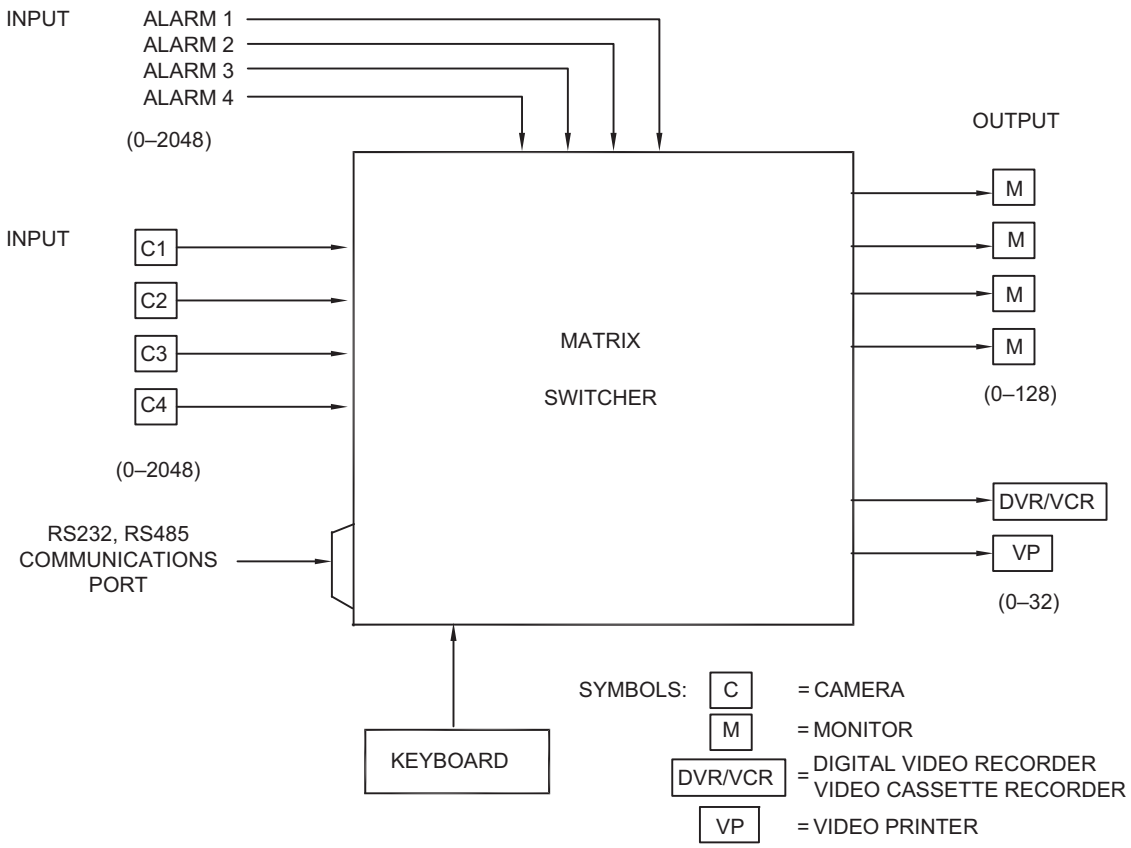


FIGURE 11-24 Microprocessor-controlled switcher and keyboard.

switcher and keyboard is used to manage these additional requirements (Figure 11-24).

In large security systems the switcher is microprocessor controlled and can switch hundreds of cameras to dozens of monitors, recorders, or video printers via an RS-232 or other communication control link. Numerous manufacturers make comprehensive keyboard-operated, computer-controlled consoles that integrate the functions of the switcher, pan/tilt pointing, automatic scanning, automatic preset pointing for pan/tilt systems, and many other functions. The power of the software-programmable console resides in its flexibility, expandability, and ability to accommodate a large variety of applications and changes in facility design. In place of a dedicated hardware system built for each specific application, this computer-controlled system can be configured via software for the application.

QUADS AND MULTIPLEXERS

A quad or a multiplexer is used when multiple camera scenes need to be displayed on one video monitor. It is interposed between the cameras and the monitor, accepts multiple camera inputs, memorizes the scenes from each camera, compresses them, and then displays multiple scenes on a single video monitor. Equipment is available to provide 2, 4, 9, 16, and up to 32 separate video scenes on one single monitor. Figure 11-25 shows a block diagram of quad and multiplexer systems.

The most popular presentation is the quad screen showing four pictures. This presentation

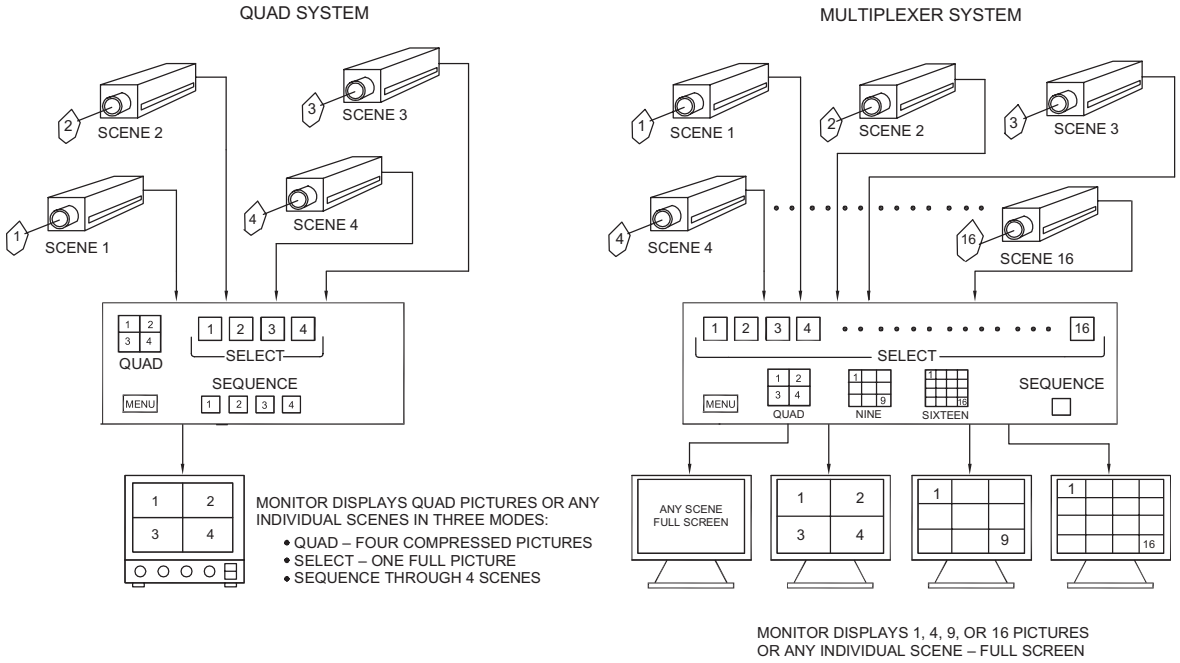


FIGURE 11-25 Quad and multiplexer block diagrams.

significantly improves camera viewing ability in multicamera systems, decreases security guard fatigue, and requires three fewer monitors in a four-camera system. There is a loss of resolution when more than one scene is presented on the monitor with resolution decreasing as the number of scenes increases. One-quarter of the resolution of a full screen is obtained on a quad display (half in horizontal and half in vertical). Quads and multiplexers have front panel controls so that: (1) a full screen image of a camera can be selected, (2) multiple cameras can be displayed (quad, nine, etc.), or (3) the full screen images of all cameras can be sequentially switched with dwell times for each camera, set by the operator.

MONITORS

Video monitors can be divided into several categories: (1) monochrome, (2) color, (3) CRT, (4) LCD, (5) plasma, and (6) computer display. Contrary to a popular misconception, larger video monitors do not necessarily have better picture resolution or the ability to increase the amount of intelligence available in the picture. All U.S. NTSC security monitors have 525 horizontal lines, therefore, the vertical resolution is about the same regardless of the CRT monitor size. The horizontal resolution is determined by the system bandwidth. With the NTSC limitation the best picture quality is obtained by choosing a monitor with resolution equal to or better than the camera or transmission link bandwidth. With the use of a higher resolution computer monitor and corresponding higher resolution camera and commensurate bandwidth to match, higher resolution video images are obtained. Figure 11-26 shows representative examples of video monitors.

Monochrome

Until the late 1990s the most popular monitor used in CCTV systems was the monochrome CRT monitor. It is still used and is available in sizes ranging from a 1-inch diagonal viewfinder to a large 27-inch diagonal CRT. By far the most popular monochrome monitor size is the 9-inch diagonal that optimizes video viewing for a

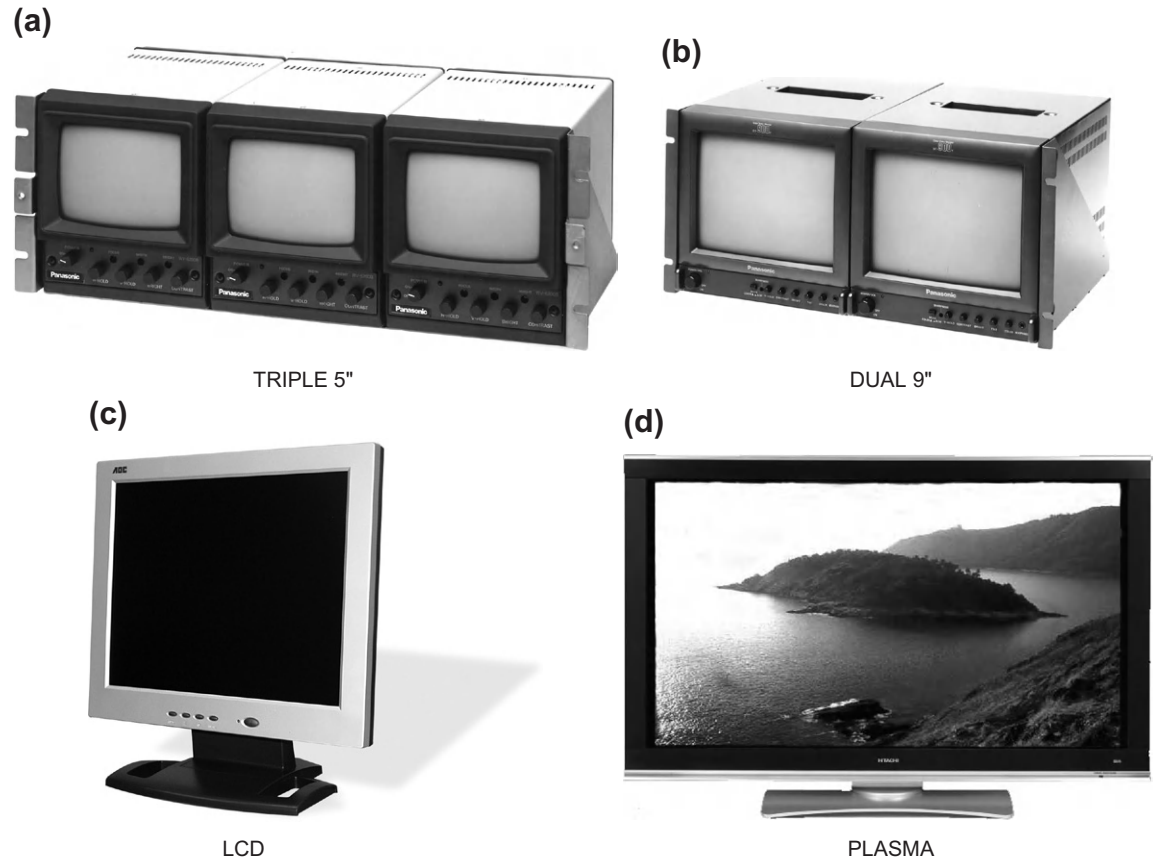


FIGURE 11-26 Standard 5- and 9-inch single/multiple CRT, LCD, and plasma monitors.

person seated about 3 feet away. A second reason for its popularity is that two of these monitors fit into the standard EIA 19-inch wide rack-mount panel. Figure 11-26(b) shows two 9-inch monitors in a dual rack–mounted version. A triple rack–mounted version of a 5-inch diagonal monitor is used when space is at a premium. The triple rack–mounted monitor is popular, since three fit conveniently into the 19-inch EIA rack. The optimum viewing distance for the triple 5-inch diagonal monitor is about 1.5 feet.

Color

Color monitors are now in widespread use and range in size from a 3- to 27-inch diagonal and have required viewing distances and capabilities similar to those of monochrome monitors. Since color monitors require three different colored dots to produce one pixel of information on the monitor, they have lower horizontal resolution than monochrome monitors. Popular color monitor sizes are 13-, 15-, and 17-inch diagonal.

CRT, LCD, Plasma, Displays

The video security picture is displayed on three basic types of monitor screens: (1) CRT, (2) LCD, and, most recently, (3) the plasma display. The analog CRT has seen excellent service from the inception of video and continues as a strong contender providing a low-cost, reliable security monitor. The digital LCD monitor is growing in popularity because of its smaller size (smaller

depth)—2–3 inches versus 12–20 inches for the CRT. The LCD is an all solid-state display that accepts the VGA computer signal. Most small (3- to 10-inch diagonal) and many large (10- to 17-inch diagonal) LCD monitors also accept an analog video input. The most recent monitor entry into the security market is the digital plasma display. This premium display excels in resolution and brightness and viewing angle and produces the highest quality image in the industry. It is also the most expensive. Screen sizes range from 20 to 42 inches diagonal. Overall depths are small and range in size from 3 to 4 inches. They are available in 4:3 and HDTV 16:9 format.

Audio/Video

Many monitors have a built-in audio channel with speakers to produce audio and video simultaneously.

RECORDERS

The video camera, transmission means, and monitor provide the remote eyes for the security guard, but as soon as the action or event is over the image disappears from the monitor screen forever. When a permanent record of the live video scene is required a VCR, DVR, network video recorder (NVR), or optical disk recorder is used (Figure 11-27).

The video image can be recorded in real time, near real time, or TL. The VCRs record the video signal on a magnetic tape cassette with a maximum real-time recording time of 6 hours and near real time of 24 hours. When extended periods of recording are required (longer than the 6-hour real-time cassette), a TL recorder is used. In the TL process the video picture is not recorded continuously (real time), but rather "snapshots" are recorded. These snapshots are spread apart in time by a fraction of a second or even seconds so that the total elapsed time for the recording can extend for hundreds of hours. Some present TL systems record over an elapsed time of 1,280 hours.

The DVR records the video image on a computer magnetic hard drive (HD) and the optical disk storage on optical disk media. The DVR and optical disk systems have a significant advantage over the VCR with respect to retrieval time of a particular video frame. VCRs take many minutes to fast forward or fast rewind the magnetic tape to locate a particular frame on the tape. Retrieval times on DVRs and optical disks are typically a fraction of a second. The VCR cassette tape is transportable and the DVR and optical disk systems are available with or without removable disks. This means that the video images (digital data) can be transported to remote locations or stored in a vault for safekeeping. The removable DVR and optical disks are about the same size as VHS cassettes.

VCR

Magnetic storage media have been used universally to record the video image. The VCR uses the standard VHS cassette format. The 8-mm Sony format is used in portable surveillance equipment because of its smaller size. Super VHS and Hi-8 formats are used to obtain higher resolution. VCRs can be subdivided into two classes: real time and TL. The TL recorder has significantly

FIGURE 11-27 DVR and NVR video disk storage equipment.

different mechanical and electrical features permitting it to take snapshots of a scene at predetermined (user-selectable) intervals. It can also record in real time when activated by an alarm or other input command. Real-time recorders can record up to 6 hours in monochrome or color. TL VCRs are available for recording time lapse sequences up to 720 hours.

DVR

The DVR has emerged as the new generation of magnetic recorder of choice. A magnetic HD like those used in a microcomputer can store many thousands of images and many hours of video in digital form. The rapid implementation and success of the DVR has resulted from the availability of inexpensive digital magnetic memory storage devices and the advancements made in digital signal compression techniques. Present DVRs are available in single channel and 4 and 16 channels and may be cascaded to provide many more channels.

A significant feature of the DVR is the ability to access (retrieve) a particular frame or recorded time period anywhere on the disk in a fraction of a second. The digital technology also allows many generations (copies) of the stored video images to be made without any errors or degradation of the image.

Optical Disk

When very large volumes of video images need to be recorded, an optical disk system is used. Optical disks have a much larger video image database capacity than magnetic disks given the same physical space they occupy. These disks can record hundreds of times longer than their magnetic counterparts.

HARD-COPY VIDEO PRINTERS

A hard-copy printout of a video image is often required as evidence in court, as a tool for apprehending a vandal or thief, or as a duplicate record of some document or person. The printout is produced by a hard-copy video printer, which is a thermal printer that "burns" the video image onto coated paper or an ink-jet or laser printer. The thermal technique used by many hard-copy printer manufacturers produces excellent quality images in monochrome or color. Figure 11-28 shows a monochrome thermal printer and a

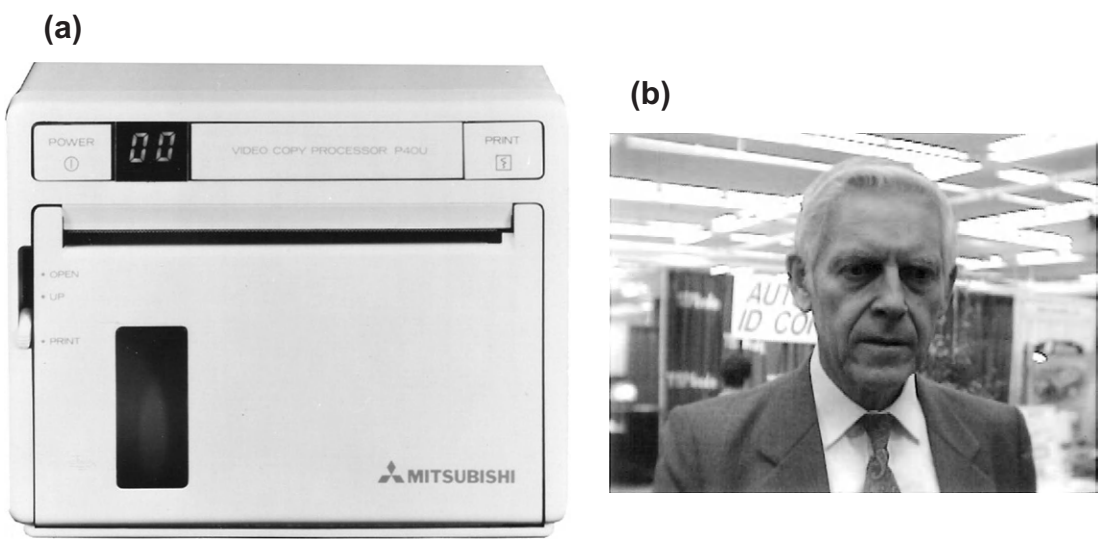


FIGURE 11-28 Thermal monochrome video printer and hard copy.

sample of the hard-copy image quality it produces. In operation, the image displayed on the monitor or played back from the recorder is immediately memorized by the printer and printed out in less than 10 seconds. This is particularly useful if an intrusion or unauthorized act has occurred and been observed by a security guard. An automatic alarm or a security guard can initiate printing the image of the alarm area or of the suspect and the printout can then be given to another guard to take action. For courtroom uses, time, date, and any other information can be annotated on the printed image.

ANCILLARY EQUIPMENT

Most video security systems require additional accessories and equipment, including: (1) camera housings, (2) camera pan/tilt mechanisms and mounts, (3) camera identifiers, (4) VMDs, (5) image splitters/inserters, and (6) image combiners. The two accessories most often used with the basic camera, monitor, and transmission link are camera housings and pan/tilt mounts. Outdoor housings are used to protect the camera and lens from vandalism and the environment. Indoor housings are used primarily to prevent vandalism and for aesthetic reasons. The motorized pan/tilt mechanisms rotate and point the system camera and lens via commands from a remote control console.

Camera Housings

Indoor and outdoor camera housings protect cameras and lenses from dirt, dust, harmful chemicals, the environment, and vandalism. The most common housings are rectangular metal or plastic products, formed from high-impact indoor or outdoor plastic, painted steel, or stainless steel (Figure 11-29). Other shapes and types include cylindrical (tube), corner-mount, ceiling-mount, and dome housings.

Standard Rectangular. The rectangular type housing is the most popular. It protects the camera from the environment and provides a window for the lens to view the scene. The housings are available for indoor or outdoor use with a weatherproof and tamper-resistant design. Options include heaters, fans, and window washers.

Dome. A significant part of video surveillance is accomplished using cameras housed in the dome housing configuration. The dome camera housing can range from a simple fixed monochrome or color camera in a hemispherical dome to a "speed-dome" housing having a high-resolution color camera with remote-controlled pan/tilt/zoom/focus. Other options include presets and image stabilization. The dome-type housing consists of a plastic hemispherical dome on the bottom half. The housing can be clear, tinted, or treated with a partially transmitting optical coating that allows the camera to see in any direction. In a freestanding application (e.g., on a pole, pedestal, or overhang), the top half of the housing consists of a protective cover and a means for attaching the dome to the structure. When the dome housing is mounted in a ceiling, a simpler housing cover is provided and mounted above the ceiling level to support the dome.

Specialty. There are many other specialty housings for mounting in or on elevators, ceilings, walls, tunnels, pedestals, hallways, and so forth. These special types include explosion-proof, bullet proof, and extreme environmental construction for arctic and desert use.

Plug and Play. In an effort to reduce installation time for video surveillance cameras, manufacturers have combined the camera, lens, and housing in one assembly ready to be mounted on a ceiling, wall, or pole and plugged into the power source and video transmission cable. These assemblies are available in the form of domes, corner mounts, ceiling mounts, and so forth, making for easy installation in indoor or outdoor applications.

Pan/Tilt Mounts

To extend the angle of coverage of a CCTV lens/camera system a motorized pan/tilt mechanism is often used. Figure 11-30 shows three generic outdoor pan/tilt types: top-mounted, side-mounted, and dome camera.

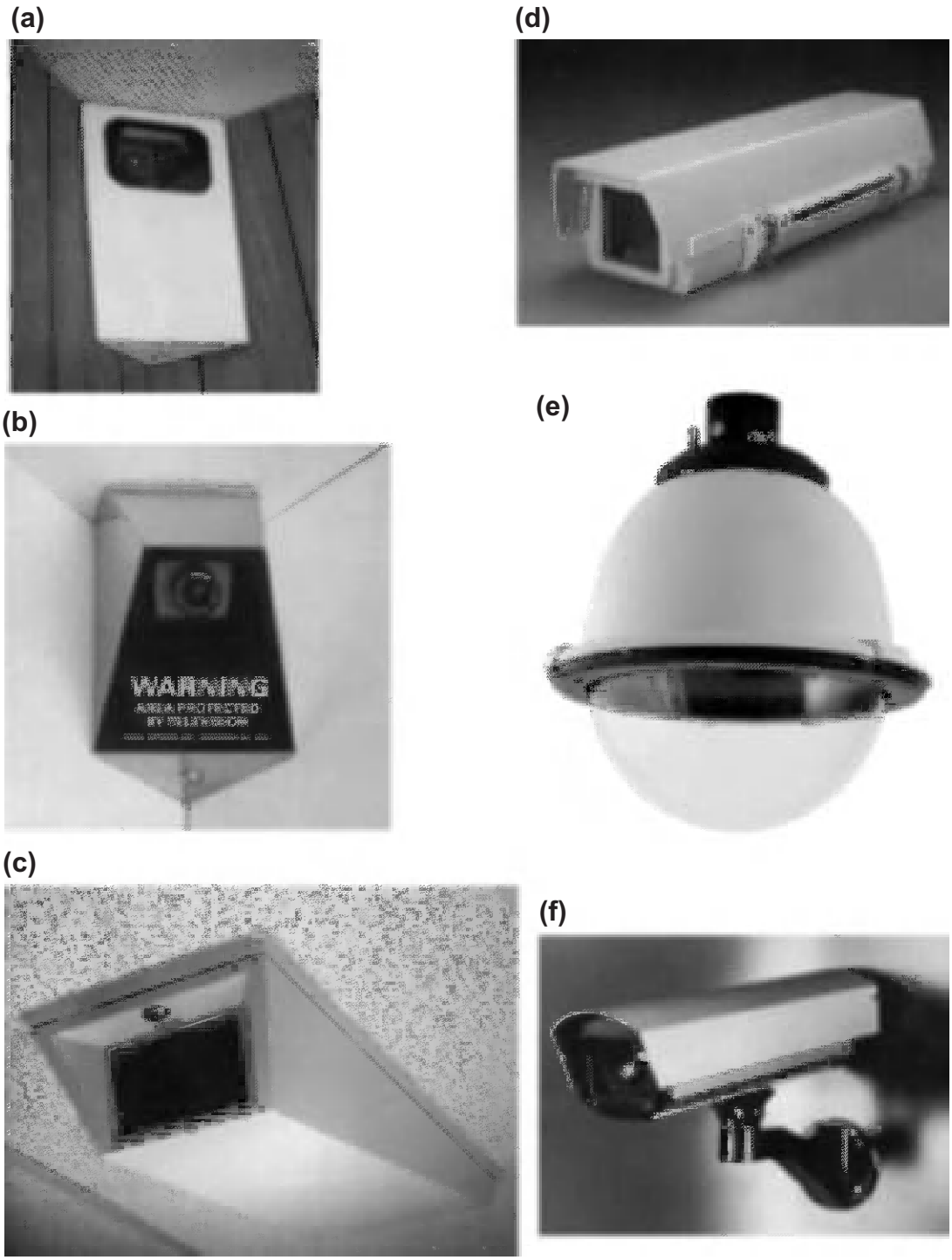


FIGURE 11-29 Standard indoor/outdoor video housings: (a) corner, (b) elevator corner, (c) ceiling, (d) outdoor environmental rectangular, (e) dome, and (f) plug and play.

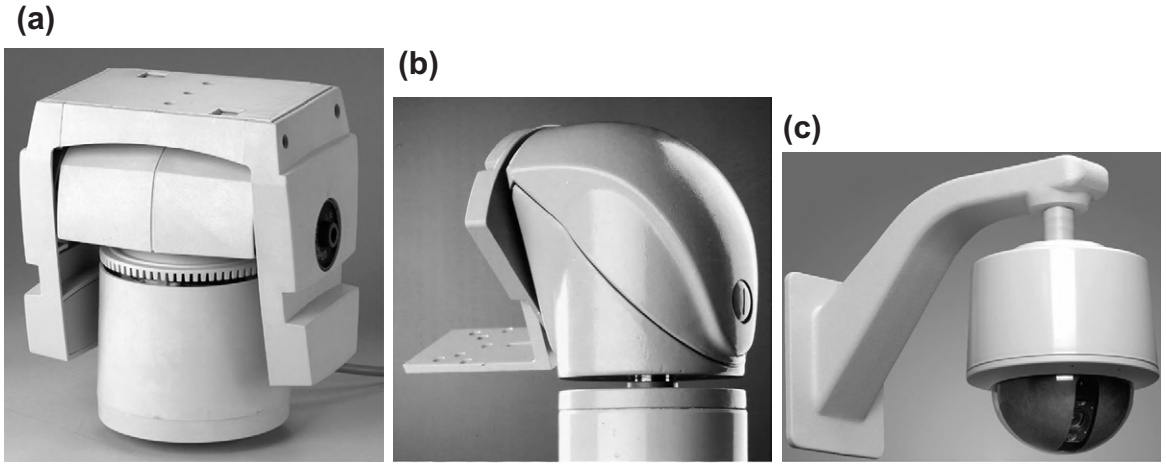


FIGURE 11-30 Video pan/tilt mechanisms.

The pan/tilt motorized mounting platform permits the camera and lens to rotate horizontally (pan) or vertically (tilt) when it receives an electrical command from the central monitoring site. Thus the camera lens is not limited by its inherent FOV and can view a much larger area of a scene. A camera mounted on a pan/tilt platform is usually provided with a zoom lens. The zoom lens varies the FOV in the pointing direction of the camera/lens from a command from the central security console. The combination of the pan/tilt and zoom lens provides the widest angular coverage for video surveillance. There is one disadvantage with the pan/tilt/zoom configuration compared with the fixed camera installation.

When the camera and lens are pointing in a particular direction via the pan/tilt platform, most of the other scene area the camera is designed to cover is not viewed. This dead area or dead time is unacceptable in many security applications, therefore, careful consideration should be given to the adequacy of their wide FOV pan/tilt design. Pan/tilt platforms range from small, indoor, lightweight units that only pan, up to large, outdoor, environmental designs carrying large cameras, zoom lenses, and large housings. Choosing the correct pan/tilt mechanism is important since it generally requires more service and maintenance than any other part of the video system.

VMD

Another important component in a video surveillance system is a VMD that produces an alarm signal based on a change in the video scene. The VMD can be built into the camera or be a separate component inserted between the camera and the monitor software in a computer. The VMD electronics, analog or digital, store the video frames, compare subsequent frames to the stored frames, and then determine whether the scene has changed. In operation the VMD digital electronics decides whether the change is significant and whether to call it an alarm to alert the guard or some equipment, or declare it a false alarm.

Screen Splitter

The electronic or optical screen splitter takes a part of several camera scenes (two, three, or more), combines the scenes, and displays them on one monitor. The splitters do not compress the image. In an *optical* splitter the image combining is implemented optically at the camera lens and requires no electronics. The *electronic*

splitter/combiner is located between the camera output and the monitor input.

Camera Video Annotation

Camera ID. When multiple cameras are used in a video system some means must be provided to identify the camera. The system uses a camera identifier component that electronically assigns an alphanumeric code and/or name to each camera displayed on a monitor, recorded on a recorder, or printed on a printer. Alphanumeric and symbol character generators are available to annotate the video signal with the names of cameras, locations in a building, and so forth.

Time and Date. When time and date is required on the video image, a time/date generator is used to annotate the video picture. This information is mandatory for any prosecution or courtroom procedure.

Image Reversal

Occasionally video surveillance systems use a single mirror to view the scene. This mirror reverses the video image from the normal left-to-right to a right-to-left (reversed image). The image reversal unit corrects the reversal.

SUMMARY

Video surveillance serves as the remote eyes for management and the security force. It provides security personnel with advance notice of breaches in security, including hostile and terrorist acts, and is a part of the plan to protect personnel and assets. It is a critical subsystem for any comprehensive security plan. In this chapter an introduction to most of the current video technology and equipment has been described.

Lighting plays an important role in determining whether a satisfactory video picture will be obtained with monochrome and color cameras and LLL ICCD cameras. Thermal IR cameras are insensitive to light and only require temperature differences between the target and the background.

There are many types of lenses available for video systems: FFL, varifocal, zoom, pinhole, panoramic, and so forth. The varifocal and zoom lenses extend the FOV of the FFL lens. The panoramic 360° lens provides entire viewing of the scene. The proper choice of lens is necessary to maximize the intelligence obtained from the scene.

Many types of video cameras are available, such as color, monochrome (with or without IR illumination), LLL intensified, thermal IR, analog and digital, simple and full featured, and daytime and nighttime. There are cameras with built-in VMD to alert security guards and improve their ability to detect and locate personnel and be alerted to activity in the scene.

An important component of the video system is the analog or digital video signal transmission means from the camera to the remote site and to the monitoring and recording site. Hard wire or fiber optics is best if the situation permits. Analog works for short distances and digital for long distances. The Internet works globally.

In multiple camera systems the quad and multiplexers permit multicamera displays on one monitor. Fewer monitors in the security room can improve guard performance.

The CRT monitor is still a good choice for many video applications. The LCD is the solid-state digital replacement for the CRT. The plasma display provides an all solid-state design that has the highest resolution and brightness and largest viewing angle, but at the highest cost.

Until about the year 2000 the only practical means for recording a permanent image of the scene was the VCR real-time or TL recorder. Now, new and upgraded systems replace the VCR with the DVR recorder with its increased reliability and fast search and retrieval capabilities to distribute the recorded video over a LAN, WAN, intranet, or Internet or wirelessly with WiFi using one of the 802.11 protocols.

Thermal, ink-jet, and laser hard-copy printers produce monochrome and color prints for immediate picture dissemination and permanent records for archiving.

All types of camera/lens housings are available for indoor and outdoor applications. Specialty

cameras/housings are available for elevators, stairwells, public facilities, casinos, shopping malls, extreme outdoor environments, and so forth.

Pan/tilt assemblies for indoor and outdoor scenarios significantly increase the overall FOV of the camera system. Small, compact speed domes have found widespread use in many indoor and outdoor video surveillance environments.

Plug-and-play surveillance cameras permit quick installation and turn-on and are available in almost every housing configuration and camera type.

The video components summarized above are used in most video security applications including: (1) retail stores, (2) manufacturing plants, (3) shopping malls, (4) offices, (5) airports, (6) seaports, (7) bus and rail terminals, and (8) government facilities. There is widespread use of small video cameras and accessories for temporary covert applications. The small size and ease of deployment of many video components and the flexibility in transmission means over short and long distances has made rapid deployment equipment for portable personnel protection systems practical and important. It is clear that the direction the video security industry is taking is the integration of the video security function with digital computing technology and the other parts of the security system: access control, intrusion alarms, fire, and two-way communications. Video security is rapidly moving from the legacy analog technology to the digital automatic video surveillance (AVS) technology.

GLOSSARY FOR CCTV

Many terms and definitions used in the security industry are unique to CCTV surveillance; others are derived from the electro-optical-optical and information-computer industries. This comprehensive glossary will help the reader better understand the literature, interpret manufacturers' specifications, and write bid specifications and requests for quotation. These terms encompass the OCTV, physical computer and communications industries, basic physics, electricity, mechanics, and optics.

access control Used to control overall access, people's assets to a building complex, schools, and even transportation companies.

analog signal Representation of data by continuously variable quantities in digital format as opposed to a finite number of discrete quantities. The electrical signal that varies continuously, and does not have discrete values.

analog television The "standard" television broadcast. Analog signals vary continuously representing fluctuations in color and brightness of a visual scent.

aperture Opening that will pass light, electrons, or other forms of radiation. In an electron gun, the aperture determines the size of, and has an effect on, the shape of the electron beam. In television optics, the aperture is the effective diameter of the lens that controls the amount of light reaching the image sensor.

automatic-iris control Electro-optic accessory to a lens that measures the video level of the camera and opens and closes the iris diaphragm to compensate for light changes.

automatic light control Process by which the illumination incident upon the face of a pickup device is automatically adjusted as a function of scent brightness.

bandwidth Data-carrying capacity of a device or network connection. The number of hertz (cycles per second) expresses the difference between the lower and upper limiting frequencies of a frequency band. Also, the width of a band of frequencies.

cable A number of electrical conductors (wires) bound in a common sheath. These may be video, data, control, or voice cables. They may also take the form of coaxial or fiber optic cables.

camera format Video cameras have 1/6-, 1/4-, 1/3-, 1/2-, and 2/3-inch sensor image formats. The actual scanned areas used on the sensors are 3.2 h×2.4 mm vertical for the 1/4 inch, 4.8 h×3.6 mm v for the 1/3 inch, 6.4 horizontal×4.8 mm vertical for the 1/2 inch, and 8.8 h×6.6 mm v for the 2/3 inch.

camera housing Enclosure designed to protect the video camera from tampering or theft when indoors or outdoors or from undue environmental exposure when placed outdoors.

camera, television Electronic device containing a solid-state sensor or an electronic image tube and processing electronics. The image formed by a lens ahead of the sensor is clocked out for a solid-state sensor or rapidly scanned by a moving electron beam in a tube camera. The sensor signal output varies with the local brightness of the image on the sensor. These variations are transmitted to a CRT, LCD, or other display device, where the brightness of the scanning spot is controlled. The scanned location (pixel) at the camera and the scanned spot at the display are accurately synchronized.

camera tube Electron tube that converts an optical image into an electrical current by a scanning process. Also called a pickup tube or television camera tube.

candle power (cp) Light intensity expressed in candles. One foot-candle (fc) is the amount of light emitted by a standard candle at a 1-foot distance.

closed-circuit television (CCTV) Closed television system used within a building or used on the exterior of a building or complex to visually monitor a location or activity for security or industrial purposes. CCTV does not broadcast consumer TV signals, but transmits in analog or digital form over a closed circuit via an electrically conducting cable, fiber optic cable, or wireless transmission. **CCTV monitor** is part of the CCTV system that receives the picture from the CCTV camera and displays it. **CCTV's role in security (psychological)** includes:

1. Serves as a deterrent
2. Records as a witness various events
3. Recognition and detection
4. Connect active usage
5. Capable of watching many areas at same time
6. Records and transmits
7. Camera can pan and tilt, zoom, and be in color
8. ROI makes it worthwhile

covert surveillance In television security, the use of camouflaged (hidden) lenses and cameras for the purpose of viewing a scene without being seen.

digital 8 Sony format that uses Hi-8 or 8-mm tapes to store digital video.

digital signal Video signal that is comprised from bits of binary data, otherwise known as ones and zeros (1, 0). The video signal travels from the point of its inception to the place where it is stored, and then on to the place where it is displayed as an analog or digital presentation.

fiber optic bundle, coherent Optical component consisting of many thousands of hair-like fibers coherently assembled so that an image is transferred from one end of the bundle to the other. The length of each fiber is much greater than its diameter. The fiber bundle transmits a picture from one end of the bundle to the other, around curves, and into otherwise inaccessible places by a process of total internal reflection. The positions of all fibers at both ends are located in an exact one-to-one relationship with each other.

fiber optic transmission Process in which light is transmitted through a long, transparent, flexible fiber, such as glass or plastic, by a series of internal reflections. For video, audio, or data transmission over long distances (thousands of feet, many miles) the light is modulated and transmitted over a single fiber in a protective insulating jacket. For light *image* transmission closely packed bundles of fibers can transmit an entire coherent image where each single fiber transmits one component of the whole image.

fiberscope Bundle of systematically arranged fibers that transmits a monochrome or full-color image that remains undisturbed when the bundle is bent. By mounting an objective lens on one end of the bundle and a relay or magnifying lens on the other, the system images remote objects onto a sensor.

foot-candle (fc) Unit of illuminance on a surface 1 square foot in area on which there is incident light of 1 lumen. The illuminance of a surface placed 1 foot from a light source that has a luminous intensity of 1 candle.

foot-lambert A measure of reflected light in a 1-foot area. A unit of luminance equal to 1 candela per square foot or to the uniform luminance at a perfectly diffusing surface emitting or reflecting light at the rate of 1 lumen per square foot.

H.264 Powerful MPEG compression algorithm standard developed through the combined effort of the ITU and MPEG organizations

providing excellent compression efficiency and motion detection attributes.

Internet Protocol (IP) Method by which data are sent from one computer to another over the Internet. Each computer, known as a host on the Internet, has one address that uniquely identifies it from all other computers on the Internet. A Web page or an e-mail is sent or received by dividing it into blocks called packets. Each packet contains both the sender's Internet address and the receiver's address. Each of these packets can arrive in an order different from the order from which they were sent in. The IP just delivers them and the Transmission Control Protocol (TCP) puts them in the correct order. The most widely used version of the IP is IP Version 4 (IPv4).

IP address On the Internet each computer and connected appliance, (camera switcher, router, etc.) must have a unique address. This series of numbers functions similarly to a street address, identifying the location of both sender and recipient for information dispatched over the computer network. The IP address has 32 bits in an 8-bit quad format. The four groups in decimal format are separated by a period (.). The quad groups represent the network and the machine or host address. An example of an IP address is 124.55.19.64.

iris Adjustable optical-mechanical aperture built into a camera lens to permit control of the amount of light passing through the lens.

iris diaphragm Mechanical device within a lens used to control the size of the aperture through which light passes. A device for opening and closing the lens aperture to adjust the f-stop of a lens.

ISO Worldwide federation of national standards bodies from over 130 countries to promote the worldwide standardization of goods and services. The ISO has international agreements that are published as international standards. The scope of ISO covers all technical fields except electrical and electronic engineering, which is the responsibility of IEC. Among well-known ISO standards is the ISO 9000 business standard that provides a framework for quality management and quality assurance.

Joint Photographic Experts Group (JPEG) Standard group that defined a compression algorithm commonly called JPEG that is used to compress data in portrait or still video images. The JPEG file format is the ISO standard 10918 that includes 29 distinct coding processes. Not all must be used by the implementer. The JPEG file type used with the GIF format is supported by the WWW protocol, usually with the file suffix "jpg."

lens Transparent optical component consisting of one or more optical glass elements with surfaces curved (usually spherical) so that they converge or diverge the transmitted rays of an object, thus forming a real or virtual image of that object.

lens, Fresnel Figuratively, a lens that is cut into narrow rings and flattened out. In practice, it is a thin plastic lens that has narrow concentric rings or steps, each acting to focus radiation into an image.

lens system Two or more lenses arranged to act in conjunction with one another.

local area network (LAN) Digital network or group of network segments confined to one building or campus. Consists of a series of PCs that have been joined together via cabling so that resources can be shared, including file and print services.

liquid crystal display (LCD) Solid-state video display created by sandwiching an electrically reactive substance between two electrodes. LCDs can be darkened or lightened by applying and removing power. Large numbers of LCD pixels grouped closely together act as pixels in a flat-panel display.

M-JPEG (motion J-PEG) Digital video compression format developed from JPEG, a compression standard for still images. When JPEG is extended to a sequence of pictures in the video stream it becomes M-JPEG.

monitor CRT-based monochrome or color display for viewing a television picture from a camera output. The monitor does not incorporate a VHF or UHF tuner and channel selector and displays the composite video signal directly from the camera, DVR, VCR, or any special effects generator. Monitors take the form of a CRT, LCD, or plasma.

multiplexer High-speed electronic switch that combines two or more video signals into a single channel to provide full-screen images up to 16 or 32 displayed simultaneously in split image format. Multiplexers can play back

everything that happened on any one camera without interference from the other cameras on the system.

pan and tilt Camera-mounting platform that allows movement in both the azimuth (pan) and the elevation (tilt) planes.

pan, panning Rotating or scanning a camera around a vertical axis to view an area in a horizontal direction.

pixel Short for picture element. Any segment of a scanning line, the dimension of which along the line is exactly equal to the nominal line width. A single imaging unit that can be identified by a computer.

radio frequency (RF) Frequency at which coherent electromagnetic radiation of energy is useful for communication purposes. The entire range of such frequencies includes the AM and FM radio spectra and the VHF and UHF television spectra.

time lapse recorder Video cassette recorder that extends the elapsed time over which it records by recording user-selected samples of the video fields or frames instead of recording in real time. For example, recording every other field produces a 15 field per second recording and doubles the elapsed time recorded on the tape. Recording every 30th field produces a 1 field per second recording and provides 30 times the elapsed recording time.

WiFi wireless, fidelity The Institute of Electrical and Electronic Engineers (IEEE) 802.11 wireless standard for transmitting video images and other data over the airwaves between computers, access points, routers, or other digital video devices.

CHAPTER

12

Biometrics Characteristics

Joseph Nelson, CPP

INTRODUCTION

By definition, *biometrics* is the study of unchanging measurable biological characteristics that are unique to each individual. Four important things about biometrics:

1. Cost
2. Overall convenience
3. Secure application
4. Identity assurance

BIOMETRICS CHARACTERISTICS [1]

Biometrics characteristics are often classed in two main categories:

- **Physiological biometrics.** Features notably identified through the five senses and processed by finite calculable differences: sight (how a person looks including things like hair and eye color, teeth, or facial features), sound (the pitch of a person's voice), smell (a person's odor or scent), taste (the composition of a person's saliva or DNA), and touch (such as fingerprints or handprints).
- **Behavioral biometrics.** Based on the manner in which people conduct themselves, such as writing style, walking rhythm, typing speed, and so forth.

For any of these characteristics to be used for sustained identification encryption purposes, they must be reliable, unique, collectable, convenient, long term, universal, and acceptable.

Types of Biometrics Devices

Iris cameras. They perform *recognition* detection of a person's identity by mathematical analysis of the random patterns that are visible within the iris of an eye from some distance. It combines computer vision, pattern recognition, statistical inference, and optics.

Iris recognition. This is rarely impeded by glasses or contact lenses and can be scanned from 10 cm to a few meters away. The iris remains stable over time as long as there are no injuries, and a single enrollment scan can last a lifetime.

Fingerprints. Formed when the friction ridges of the skin come in contact with a surface that is receptive to a print by using an agent to form the print, such perspiration, oil, ink, grease, and so forth. The agent is transferred to the surface and leaves an impression which forms the fingerprint.

Hand scanner and finger reader recognition systems. These measure and analyze the overall structure, shape, and proportions of the hand, such as length, width, and thickness of the hand, fingers, and joints, and characteristics of the skin surface such as creases and ridges.

Facial recognition device. This views an image or video of a person and compares it to one in the database. It does this by comparing structure, shape, and proportions of the face; distance between the eyes, nose, mouth, and jaw; upper outlines of the eye sockets; the sides of the mouth; the location of the nose and eyes;

and the area surrounding the cheek bones. The main *facial recognition* methods are feature analysis, neural network, eigenfaces, and automatic face processing.

Voice recognition voiceprint. This is a spectrogram, which is a graph that shows a sound's frequency on the vertical axis and time on the horizontal axis. Different speech creates different shapes on the graph. Spectrograms also use color or shades of gray to represent the acoustical qualities of sound.

Smart card. A pocket-sized plastic card with an embedded chip that can process data. It is used in industries such as health care, banking, government, and *biometrics*. Smart cards can process data via input and output of information and are essentially mini-processors. They can provide identification, authentication, data storage, and access to buildings, bank machines, and communications and entertainment.

Digital biometrics signature. This is equivalent to a traditional *handwritten* signature in many respects since if the signature is properly implemented it is more difficult to forge than the traditional type. Digital signature schemes are *cryptographically* based and must be implemented properly to be effective. Digital signatures can be used for e-mail, contracts, or any message sent via some other *cryptographic protocol*.

Vein recognition. Vein recognition is a type of biometrics that can be used to identify individuals based on the vein patterns in the human finger.

REFERENCE

[1] Biometrics characteristics, available at www.findBiometrics.com, 2012.

CHAPTER

13

Access Control and Badges

Joseph Nelson, CPP

ACCESS CONTROL

Perimeter barriers, intrusion-detection devices, and protective lighting provide physical-security safeguards; however, they alone are not enough. An access control system must be established and maintained to preclude unauthorized entry. Effective access control procedures prevent the introduction of harmful devices, materiel, and components. They minimize the misappropriation, pilferage, or compromise of materiel or recorded information by controlling packages, materiel, and property movement. Access control rosters, personal recognition, ID cards, badge-exchange procedures, and personnel escorts all contribute to an effective access control system.

DESIGNATED RESTRICTED AREAS

The installation commander is responsible for designating and establishing restricted areas. A restricted area is any area that is subject to special restrictions or controls for security reasons. This does not include areas over which aircraft flight is restricted. Restricted areas may be established for the following:

- The enforcement of security measures and the exclusion of unauthorized personnel.
- Intensified controls in areas requiring special protection.
- The protection of classified information or critical equipment or materials.

DEGREE OF SECURITY

The degree of security and control required depends on the nature, sensitivity, or importance of the security interest. Restricted areas are classified as controlled, limited, or exclusion areas.

- A controlled area is that portion of a restricted area usually near or surrounding a limited or exclusion area. Entry to the controlled area is restricted to personnel with a need for access. Movement of authorized personnel within this area is not necessarily controlled since mere entry to the area does not provide access to the security interest. The controlled area is provided for administrative control, for safety, or as a buffer zone for in-depth security for the limited or exclusion area. The commander establishes the control of movement.
- A limited area is a restricted area within close proximity of a security interest. Uncontrolled movement may permit access to the item. Escorts and other internal restrictions may prevent access within limited areas.
- An exclusion area is a restricted area containing a security interest.

Access Control

Uncontrolled movement permits direct access to the item. The security protection afforded by a restricted area pertains particularly to subversive-activity control, that is, protection against

espionage, sabotage, or any such action adversely affecting national defense. Within this context, the designation "restricted area" is not applicable to an area solely for protection against common pilferage or misappropriation of property or material that is not classified or not essential to national defense. For example, an area devoted to the storage or use of classified documents, equipment, or materials should be designated as a restricted area to safeguard against espionage. An installation communications center should also be so designated to safeguard against sabotage. On the other hand, a cashier's cage or an ordinary mechanic's tool room should not be so designated, although the commander may impose controls to access. This may be a simple matter of posting an "off limits to unauthorized personnel" sign.

A restricted area must be designated in writing by the management and must be posted with warning signs. In areas where English is one of two or more languages commonly spoken, warning signs will be posted in English and in the local language.

An installation may have varying degrees of security. It may be designated in its entirety as a restricted area, with no further restrictions, or it may be subdivided into controlled, limited, or exclusion areas with restrictions of movement and specific clear zones, depicting a simplified restricted area and the degrees of security.

CONSIDERATIONS

There are other important considerations concerning restricted areas and their lines of division. These considerations include the following:

- **A survey and analysis of the installation, its missions, and its security interests.** This can determine immediate and anticipated needs that require protection. Anticipated needs are determined from plans for the future.
- **The size and nature of the security interest being protected.** Safes may provide adequate protection for classified documents and small items; however, large items may have to be placed within guarded enclosures.
- **Some security interests are more sensitive to compromise than others.** Brief observation or a simple act by an untrained person may constitute a compromise in some cases. In others, detailed study and planned action by an expert may be required.
- **All security interests should be evaluated according to their importance.** This may be indicated by a security classification such as confidential, secret, or top secret.

Access Control

- Parking areas for privately owned vehicles (POVs) are established outside of restricted areas. Vehicle entrances must be kept at a minimum for safe and efficient control.
- Physical protective measures (such as fences, gates, and window bars) must be installed.

EMPLOYEE SCREENING

Screening job applicants to eliminate potential acts of espionage and sabotage and other security risks is important in peacetime and is critical during a national emergency. Personnel screenings must be incorporated into standard personnel policies.

An applicant should be required to complete a personnel security questionnaire, which is then screened for completeness and used to eliminate undesirable applicants. A careful investigation should be conducted to ensure that the applicant's character, associations, and suitability for employment are satisfactory. The following sources may be helpful in securing employment investigative data:

- State and local police (including national and local police in overseas areas)
- Former employers
- Public records
- Credit agencies
- Schools (all levels)
- References. (These references should include those names not furnished by the applicant. These are known as throw-offs, and they are

obtained during interviews of references furnished by applicants.)
- Others as appropriate, including the FBI, the U.S. Army Criminal Records Repository, and the Defense Investigative Agency.

Medical screening considerations should be made (based on an applicant's position, such as a guard) to evaluate physical and mental stamina. Once an applicant has been identified for employment, he is placed on an access control roster.

IDENTIFICATION SYSTEM

An ID system is established at each installation or facility to provide a method of identifying personnel. The system provides for personal recognition and the use of security ID cards or badges to aid in the control and movement of personnel activities.

Standard ID cards are generally acceptable for access into areas that are unrestricted and have no security interest. Personnel requiring access to restricted areas should be issued a security ID card or badge. The design of the card/badge must be simple and provide for adequate control of personnel.

A security ID card/badge system must be established for restricted areas with 30 or more employees per shift.

ID METHODS

Four of the most common access control ID methods are the personal-recognition system, the single-card/badge system, the card or badge-exchange system, and the multiple-card/badge system.

Personal-Recognition System

The personal-recognition system is the simplest of all systems. A member of the security force providing access control visually checks the person requesting entry. Entry is granted based on:

- The individual being recognized.
- The need to enter being established.
- The person being on an access control roster.

Single-Card/Badge System

This system reflects permission to enter specific areas by the badge depicting specific letters, numbers, or particular colors. This system lends to comparatively loose control and is not recommended for high-security areas. Permission to enter specific areas does not always go with the need to know. Because the ID cards/badges frequently remain in the bearer's possession while off duty, it affords the opportunity for alteration or duplication.

Card/Badge-Exchange System

In this system, two cards/badges contain identical photographs. Each card/badge has a different background color, or one card/badge has an overprint. One card/badge is presented at the entrance to a specific area and exchanged for the second card/badge, which is worn or carried while in that area. Individual possession of the second card/badge occurs only while the bearer is in the area for which it was issued. When leaving the area, the second card/badge is returned and maintained in the security area. This method provides a greater degree of security and decreases the possibility of forgery, alteration, or duplication of the card/badge. This level of protection requires multiple access control elements as the levels of protection increase. In the case of the badge exchange, this system counts as two access control elements.

Multiple-Card/Badge System

This system provides the greatest degree of security. Instead of having specific markings on the cards/badges denoting permission to enter various restricted areas, the multiple-card/badge system makes an exchange at the entrance to each security area. The card/badge information is identical and allows for comparisons. Exchange cards/badges are maintained at each area only for individuals who have access to the specific area.

MECHANIZED/AUTOMATED SYSTEMS

An alternative to using security officers to visually check cards/badges and access rosters is to use building card-access systems or biometric-access readers. These systems can control the flow of personnel entering and exiting a complex. Included in these systems are:

- Coded devices such as mechanical or electronic keypads or combination locks.
- Credential devices such as magnetic stripe or proximity card readers.
- Biometric devices such as fingerprint readers or retina scanners.

Access control and ID systems base their judgment factor on a remote capability through a routine discriminating device for positive ID. These systems do not require security officers at entry points; they identify an individual in the following manner:

- The system receives physical ID data from an individual.
- The data are encoded and compared to stored information.
- The system determines whether access is authorized.
- The information is translated into readable results.

Specialized mechanical systems are ideal for highly sensitive situations because they use a controlled process in a controlled environment to establish the required database and accuracy. One innovative technique applied to ID and admittance procedures involves dimension comparisons. The dimension of a person's full hand is compared to previously stored data to determine entry authorization. Other specialized machine readers can scan a single fingerprint or an eye retina and provide positive ID of anyone attempting entry.

An all-inclusive automated ID and access control system reinforces the security in-depth ring through its easy and rapid change capability. The computer is able to do this through its memory. Changes can be made quickly by the system's administrator.

The commercial security market has a wide range of mechanized and automated hardware and software systems. Automated equipment is chosen only after considering the security needs and the environment in which it operates. These considerations include whether the equipment is outdoors or indoors, the temperature range, and weather conditions. Assessment of security needs and the use of planning, programming, and budgeting procedures greatly assist a security manager in improving the security posture.

CARD/BADGE SPECIFICATIONS

Security cards/badges should be designed and constructed to meet the necessary requirements. Upon issuing a card/badge, security personnel must explain to the bearer the wear required and the authorizations allowed with the card/badge. This includes:

- Designation of the areas where an ID card/badge is required.
- A description of the type of card/badge in use and the authorizations and limitations placed on the bearer.
- The required presentation of the card/badge when entering or leaving each area during all hours of the day.
- Details of when, where, and how the card/badge should be worn, displayed, or carried.
- Procedures to follow in case of loss or damage of the card.
- The disposition of the card/badge upon termination of employment, investigations, or personnel actions.
- Prerequisites for reissuing the card/badge.

VISITOR IDENTIFICATION AND CONTROL

Procedures must be implemented to properly identify and control personnel. This includes visitors presenting their cards/badges to guards at entrances of restricted areas. Visitors are required

to stay with their assigned escort. Guards must ensure that visitors stay in areas relating to their visit; an uncontrolled visitor, although conspicuously identified, could acquire information for which he is not authorized. Foreign-national visitors should be escorted at all times.

Approval for visitors should be obtained at least 24 hours in advance (if possible). Where appropriate, the installation should prepare an agenda for the visitor and designate an escort officer. Measures must be in place to recover visitor cards/badges on the visit's expiration or when they are no longer required.

Physical-security precautions against pilferage, espionage, and sabotage require the screening, ID, and control of visitors. Further information about visiting requirements and procedures should be in your policy and procedures.

Visitors are generally classed in the following categories:

- Persons with whom every installation or facility has business (such as suppliers, customers, insurance inspectors, and government inspectors).
- Individuals or groups who desire to visit an installation or facility for personal or educational reasons. Such visits may be desired by educational, technical, or scientific organizations.
- Individuals or groups specifically sponsored by the government (such as foreign nationals visiting under technical cooperation programs and similar visits by U.S. nationals). Requests for visits by foreign nationals must be processed according to policy and procedures.
- Guided tours to selected portions of the installation in the interest of public relations.

The ID and control mechanisms for visitors must be in place. They may include the following:

- Methods of establishing the authority for admitting visitors and any limitations relative to access.
- Positive ID of visitors by personal recognition, visitor permit, or other identifying credentials. Contact the employer, supervisor, or officer in charge to validate the visit.
- The use of visitor registration forms. These forms provide a record of the visitor and the time, location, and duration of his visit.
- The use of visitor ID cards/badges. The cards/badges bear serial numbers, the area or areas to which access is authorized, the bearer's name, and escort requirements.

Individual groups entering a restricted area must meet specific prerequisites before being granted access. The following guidance is for group access into a restricted area.

VISITORS

Before allowing visitors into a restricted area, contact the person or activity being visited. After verifying the visitor's identity, issue a badge, complete the registration forms, and assign an escort (if required). Visitors may include public-utility and commercial-service representatives.

Very Important Persons

The procedures for admitting very important persons (VIPs) and foreign nationals into restricted areas should be in your policy manual. Special considerations and coordination with the protocol office are necessary. A 24-hour advance notice is desirable for these requests, along with an agenda for the visit and the designation of an escort, if appropriate.

Civilians Working on Jobs under Government Contract

To allow these personnel to conduct business in restricted areas, the security manager must coordinate with the procurement office. The security manager must also identify movement-control procedures for these employees.

Cleaning Teams

Supervisors using cleaning teams must seek technical advice from the physical-security office on

internal controls for each specific building. This may include providing escorts.

Department of Defense Employees in Work Areas after Normal Operating Hours

Supervisors establish internal controls based on coordination with the security manager. They also notify security personnel of the workers' presence, type, and duration of work.

ENFORCEMENT MEASURES

The most vulnerable link in any ID system is its enforcement. Security forces must be proactive in performing their duties. A routine performance of duty will adversely affect even the most elaborate system. Positive enforcement measures must be prescribed to enhance security. Some of these measures may include the following.

Access Control

- Designating alert and tactful security personnel at entry control points.
- Ensuring that personnel possess quick perception and good judgment.
- Requiring entry-control personnel to conduct frequent irregular checks of their assigned areas.
- Formalizing standard procedures for conducting guard mounts and posting and relieving security personnel. These measures will prevent posting of unqualified personnel and a routine performance of duty.
- Prescribing a uniform method of handling or wearing security ID cards/badges. If carried on the person, the card must be removed from the wallet (or other holder) and handed to security personnel. When worn, the badge will be worn in a conspicuous position to expedite inspection and recognition from a distance.
- Designing entry and exit control points of restricted areas to force personnel to pass in a single file in front of security personnel. In some instances, the use of turnstiles may be advisable to assist in maintaining positive control.
- Providing lighting at control points. The lighting must illuminate the area to enable security personnel to compare the bearer with the ID card/badge.
- Enforcing access control measures by educating security forces and employees. Enforcement of access control systems rests primarily with the security forces; however, it is essential that they have the full cooperation of the employees. Employees must be instructed to consider each unidentified or improperly identified individual as a trespasser. In restricted areas where access is limited to a particular zone, employees must report unauthorized individuals to the security force.
- Positioning ID card/badge racks or containers at entry control points so they are accessible only to guard-force personnel.
- Appointing a responsible custodian to accomplish control procedures of cards/badges according to policy manual. The custodian is responsible for the issue, turn in, recovery, and renewal of security ID cards/badges as well as monthly verification of individuals in various areas and the deletion of terminated employee badges.

The degree of compromise tolerable in the ID system is in direct proportion to the degree of security required. The following control procedures are recommended for preserving the integrity of a card/badge system:

- Maintenance of an accurate written record or log listing (by serial number) all cards and badges and showing those on hand, to whom they are issued, and their disposition (lost, mutilated, or destroyed).
- Authentication of records and logs by the custodian.
- A periodic inventory of records by a manager or auditors.
- The prompt invalidation of lost cards/badges and the conspicuous posting at security control points of current lists of lost or invalidated cards/badges.
- The establishment of controls within restricted areas to enable security personnel to determine the number of persons within the area.

- The establishment of the two-person rule (when required).
- The establishment of procedures to control the movement of visitors. A visitor-control record will be maintained and located at entry control points.

SIGN/COUNTERSIGN AND CODE WORD

This method of verifying identity is primarily used in a tactical environment. According to the local SOP, the sign/countersign or code-word procedures must be changed immediately if compromised.

DURESS CODE

The duress code is a simple word or phrase used during normal conversation to alert other security personnel that an authorized person is under duress. A duress code requires planning and rehearsal to ensure an appropriate response. This code is changed frequently to minimize compromise.

ACCESS CONTROL ROSTERS

Admission of personnel to a restricted area is granted to those identified and listed on an access control roster. Pen-and-ink changes may be made to the roster. Changes are published in the same manner as the original roster.

Rosters are maintained at access control points. They are kept current, verified, and accounted for by an individual designated by a manager. This manager or their designated representatives authenticate the rosters. Admission of persons other than those on the rosters is subject to specific approval by the security manager or another specific manager. These personnel may require an escort according to the local SOP.

CONTROL METHODS

There are a number of methods available to assist in the movement and control of personnel in limited, controlled, and restricted areas. The following paragraphs discuss the use of escorts and the two-person rule.

Escorts

Escorts are chosen because of their ability to accomplish tasks effectively and properly. They possess knowledge of the area being visited. Escorts may be guard-force personnel, but they are normally personnel from the area being visited. Local regulations and SOPs determine if a visitor requires an escort while in the restricted area. Personnel on the access list may be admitted to restricted areas without an escort.

Two-Person Rule

The two-person rule is designed to prohibit access to sensitive areas or equipment by a lone individual. Two authorized persons are considered present when they are in a physical position from which they can positively detect incorrect or unauthorized procedures with respect to the task or operation being performed. The team is familiar with applicable safety and security requirements, and they are present during any operation that affords access to sensitive areas or equipment that requires the two-person rule. When application of the two-person rule is required, it is enforced constantly by the personnel who constitute the team.

The two-person rule is applied in many other aspects of physical security operations, such as the following:

- When uncontrolled access to vital machinery, equipment, or materiel might provide opportunity for intentional or unintentional damage that could affect the installation's mission or operation.
- When uncontrolled access to funds could provide opportunity for diversion by falsification of accounts.
- When uncontrolled delivery or receipt for materials could provide opportunity for pilferage through "short" deliveries and false receipts.

The two-person rule is limited to the creativity of the PM and the physical-security manager. They should explore every aspect of physical security operations in which the two-person rule would provide additional security and assurance and

include all appropriate recommendations and provisions of the physical-security plan. An electronic-entry control system may be used to enforce the two-person rule. The system can be programmed to deny access until two authorized people have successfully entered codes or swiped cards.

SECURITY CONTROLS OF PACKAGES, PERSONAL PROPERTY, AND VEHICLES

A good package-control system helps prevent or minimize pilferage, sabotage, and espionage. The local SOP may allow the entry of packages with proper authorization into restricted areas without inspection. A package checking system is used at the entrance gate. When practical, inspect all outgoing packages except those properly authorized for removal. When a 100% inspection is impractical, conduct frequent unannounced spot checks. A good package-control system assists in the movement of authorized packages, material, and property.

Property controls are not limited to packages carried openly, and they include the control of anything that could be used to conceal property or material. Personnel should not be routinely searched except in unusual situations. Searches must be performed according to the local SOP.

All POVs on the installation should be registered with the PM or the installation's physical-security office. Security personnel should assign a temporary decal or other temporary ID tag to visitors' vehicles to permit ready recognition. The decal or the tag should be distinctly different from that of permanent-party personnel.

When authorized vehicles enter or exit a restricted area, they undergo a systematic search, including (but not limited to) the:

- Vehicle's interior
- Engine compartment
- External air breathers
- Top of the vehicle
- Battery compartment
- Cargo compartment
- Undercarriage

The movement of trucks and railroad cars into and out of restricted areas should be supervised and inspected. Truck and railroad entrances are controlled by locked gates when not in use and are manned by security personnel when unlocked. The ID cards/badges are issued to operators to ensure proper ID and registration for access to specific loading and unloading areas.

All conveyances entering or leaving a protected area are required to pass through a service gate manned by security forces. Drivers, helpers, passengers, and vehicle contents must be carefully examined. The examination may include:

- Appropriate entries in the security log (including the date, operator's name, load description, and time entered and departed).
- A check of the operator's license.
- Verification of the seal number with the shipping document and examination of the seal for tampering.

Incoming trucks and railroad cars must be assigned escorts before they are permitted to enter designated limited or exclusion areas. Commanders should establish published procedures to control the movement of trucks and railroad cars that enter designated restricted areas to discharge or pick up cargo (escorts will be provided when necessary).

The best control is provided when all of these elements are incorporated into access control procedures. Simple, understandable, and workable access control procedures are used to achieve security objectives without impeding operations. When properly organized and administered, access control procedures provide a method of positively identifying personnel who have the need to enter or leave an area.

TACTICAL-ENVIRONMENT CONSIDERATIONS

Access control procedures during tactical operations may establish additional challenges for the commander. In some instances, the commander

cannot provide a perimeter barrier (such as a fence). Managers are still required to provide security measures for restricted areas, although they may not always have the necessary assets. Early warning systems and the use of guards become crucial. A restricted area may become a requirement without prior notice during an operation. Managers must plan for these considerations when developing their budget. Funding must be requested and set aside to support physical-security requirements during tactical operations. Resources will not always be available; therefore, managers must implement procedures that support access control measures. Improvising will become common practice to overcome shortfalls concerning access control equipment in the field [1].

Building Design

When designing, building, and installing engineered security controls, security practitioners must consider a variety of factors to ensure optimum results. While not doing so can leave access control systems prone to nuisance alarms, it can also lead to limited or no authorization controls at all. Your objective should be to prevent penetration and provide authorized access through layered levels of security within your complex.

Layered Levels of Security

The outer perimeter/outer protective layer can be a man-made barrier controlling both traffic and people flow. The inner layer contains the interior lobby and main entrance, turnstiles, revolving doors, handicap gates, elevators, emergency doors alarmed, and private occupied space. The inner protective layer contains biometrics, mirrors, and closed-circuit TV (CCTV) applications. The middle layer consists of exterior parts of the building.

High-security areas are laid within the inner layer with limited access to a select few. Reducing opportunity within your complex's design must be tailored to the specific area's environment.

When designing administrative controls for access control, one must consider the tolerance for process errors. This means we should consider the percentage of unauthorized transactions we can allow with minimal consequence. While engineered controls make a significant difference controlling access capabilities, our tolerance for mistakes or errors in access control often equally relate to the administrative controls that rule the measurement of results and prove our access control levels are operating at the desired levels.

Access Cards

1. **Proximity cards.** Proximity access cards are most often used for EA systems. They work via the use of passively tuned circuits that have been embedded in a high-grade fiberglass epoxy card. One can gain access when the cardholder holds the card within two to four inches from a card reader. The reader's sensor detects the pattern of the frequencies programmed in the card, and it communicates with the sensor by electromagnetic, ultrasound, or optical transmission. This pattern is then transmitted to the system's computer. If the pattern matches that of the reader, the reader unlocks the door and records the transaction. If the pattern does not match, no access is granted and this transaction is recorded.
2. **Magnetic stripe cards.** Magnetic cards use various kinds of materials and mediums to magnetically encode digital data onto cards. To gain access the card user inserts or "swipes" (passes the badge through) the card reader. As the card is withdrawn from the reader, it moves across a magnetic head, similar to that in a tape recorder head, that reads the data programmed in the card. The information read from the card is sent to the system's computer for verification. If verification is made, the computer sends a signal to the card reader to grant or deny access, and if access is granted, the door is unlocked. Magnetic cards look like regular credit cards. The most popular medium for this type of access card is a magnetic stripe on which a pattern of digital data is

encoded. This type of card is relatively inexpensive and a large amount of data can be stored magnetically compared to other kinds of magnetic media. These cards tend to chip and break, however, through excessive use.

3. **Weigand cards.** Weigand-based access control cards use a coded pattern on magnetized wire embedded within the card. When this card is inserted into a reader, the reader's internal sensors are activated by the coded wire. This type of card is moderately priced and will handle a large amount of traffic. It is less vulnerable to vandalism and weather effects than other types of cards, but it does stand up to a considerable amount of wear and tear.
4. **Biometrics access control.** Biometrics is most accurate when using one or more fingerprints, palm prints or palm scan, hand geometry, or retina and iris scan. Remember deterrent controls delay unauthorized access. Think *proactive management.*
5. **Biometric ID systems operate locks to doors.** Used in high-security areas where limited access is maintained, this system checks physical characteristics that verify and allow access/entry.
6. **Smart cards.** These contain an integrated chip embedded in them. They have coded memories and microprocessors; hence, they are like computers. The technology in these cards offers many possibilities, particularly with proximity-card-based card access systems. Optical cards have a pattern of light spots that can be read by a specific light source, usually infrared. Capacitance cards use coded capacitor-sensitive material that is enclosed in the card. A current is induced when the card activates a reader that checks the capacitance of the card to determine the proper access code. Some access devices come in the shape of keys, disks, or other convenient formats that provide users with access tools that look attractive and subdued but at the same time are functional.
7. **Dual-technology card.** Some cards have dual technology, such as magnetic stripe/proximity card and an RFID/proximity card.
8. **Card readers.** Card readers are devices used for reading access cards. Readers come in various shapes, sizes, and configurations. The most common reader is the type where the card user inserts the card in a slot or runs or "swipes" the card through a slot. The other type of reader uses proximity technology where the card user presents or places the card on or near the reader. Some insertion-type card readers use keypads; after the user inserts the card, the user enters a unique code number on the keypad. This action then grants access.
9. **Electronic access control (EAC) systems applications.** Ideally used as part of a fully integrated facility management system. In such a system electronic access control is interfaced and integrated with fire safety/life safety systems, CCTV systems, communication systems, and nonsecurity systems such as heating, ventilation, and air conditioning (HVAC). In an integrated system, EAC systems allow users to be accessed into various areas or limited areas. They can track access and provide attendance records. As a safety feature and for emergency response situations, they can determine where persons are located in facilities. In general, EAC systems are very flexible and strides in technology have made them even more so.

This section barely covers all that you need to know about EAC. The best way to learn about EAC is to actually work with EAC systems. Take advantage of every opportunity to work with EAC systems. Seek assignments where EAC systems are used, and ask questions from control room operators, your supervisors, and EAC vendors and service technicians. There are many excellent sources where you can read about EAC and related systems.

Badges

There are many types of badges. Badges with color coding can be used for various reasons that may include designating years of service, clearance levels, departments, and/or locations. In

addition, there is video badging, which displays a corporate logo or a special design and may be color-coded, and there are badges incorporating digitized data or a photograph.

When badges are initially introduced to a complex's security system, it would appear to be a simple process, until some of the questions and concerns we have identified below arise:

1. If an employee loses their badge, it costs $10.00 to replace. Some employers allow one "free" replacement easily.
2. When an employee is fired, who retrieves the badge, keys, or other company property? Are all company badges deleted if not used in 30 days?
3. If a badge is stolen, what is the process to render it useless?
4. If a badge is borrowed or used by an unauthorized person(s), has sufficient data been included? Height, weight, and color of eyes and hair can be included by using both sides of the card.
5. Database for badges? Are managers required to give written permission before access is granted?
6. Identify access levels and authorization processes.
7. Consider all potential vulnerabilities and the risk of threats.

REFERENCE

[1] U.S. Army Field Manual, FM-3–19.30, formerly FM-19-30, Jan. 2001, Chapter 7 modified.

CHAPTER

14

Fence Standards

*Chain-Link Fence Manufacturers Institute**

RECOMMENDATIONS

Chain-link fencing has been the product of choice for security fencing for over 60 years because of its strength, corrosion resistance, "see-through capabilities," ease of installation, versatility, variety of product selection, and value. A chain-link fence is one of the primary building blocks for a facility's perimeter security system.

The physical security barrier provided by a chain-link fence provides one or more of the following functions:

- Gives notice of a legal boundary of the outermost limits of a facility.
- Assists in controlling and screening authorized entries into a secured area by deterring entry elsewhere along the boundary.
- Supports surveillance, detection, assessment, and other security functions by providing a zone for installing intrusion detection equipment and closed-circuit television (CCTV).
- Deters casual intruders from penetrating a secured area by presenting a barrier that requires an overt action to enter.
- Demonstrates the intent of an intruder by their overt action of gaining entry.
- Causes a delay to obtain access to a facility, increasing the possibility of detection.
- Creates a psychological deterrent.
- Reduces the number of security guards required and frequency of use for each post.
- Optimizes the use of security personnel while enhancing the capabilities for detection and apprehension of unauthorized individuals.
- Demonstrates a corporate concern for facility security.
- Provides a cost-effective method of protecting facilities.

SECURITY PLANNING

Chain-link fence enhances the goals of good security planning. In-depth security planning takes into consideration the mission and function, environmental concerns, threats, and the local area of the facility to be secured. This can be translated into an A-B-C-D method that points out the values of chain-link fencing to a security program.

A. AIDS to security. Chain-link fencing assists in the use of other security equipment, such as the use of intrusion detectors, access controls, cameras, and so forth. Chain-link fences can be employed as aids to protection in an exterior mode or an internal

Note: The information in this chapter has been provided as a public service to assist in the design of appropriate security fencing. The Chain-Link Fence Manufacturers Institute disclaims any responsibility for the design and operation of specific security fence systems. Permission obtained to be reproduced in 2012.

protected property, as a point protection, and for general protection as required.

B. BARRIERS for security. These can be buildings, chain-link fences, walls, temporary checkpoints, and so on.

C. CONTROLS support the physical security chain-link fences and barriers, such as an access control system tied into vehicle gates and pedestrian portals, various level identification badges and temporary badges, security escorts, and internal procedures.

D. DETERRENTS such as a chain-link fence, guards, lighting, signage, and checkpoint control procedures are a few of the deterrents that ensure intruders will consider it difficult to successfully gain access.

When properly used, the aspects of the A-B-C-D method reinforce and support each other. Thus a chain-link fence is also a deterrent, and a barrier, if need be. By combining A-B-C-D, sufficient obstacles are created to prevent an intruder from obtaining information that is being worked on during the day in the controlled access area and then is protected at night, on weekends, and on holidays through the implementation of the security in-depth concept.

More important, keep in mind that a chain-link fence is the common denominator of the A-B-C-D system and will reduce overall risk, secure the environment, and reduce security costs if designed and installed properly. However, believing that a fence will eliminate all illegal access is not prudent. A fence system will only delay or reduce intrusion.

To ensure the effectiveness of the facility security fence program, it is recommended that a maintenance program be developed for the proper maintenance of the fence system, gates, gate operators, and related access controls.

MATERIAL SPECIFICATIONS

Material specifications for chain-link fence are listed in the following:

- *Chain-Link Fence Manufacturers Institute Product Manual* (CLFMI)
- American Society of Testing Materials (ASTM), volume 01.06
- Federal Specification RR-F-191 K/GEN, May 14, 1990
- ASTM F 1553, "The Standard Guide for Specifying Chain-Link Fence," provides the appropriate information to develop a specification document

Framework

The framework for a chain-link fence consists of the line posts, end posts, corner posts, gateposts, and, if required, a top, mid, bottom, or brace rail. The Federal Specification and the CLFMI "Wind Load Guide for the Selection of Line Post Spacing and Size" provide recommended post sizes for the various fence heights. However, the latter document also provides choices of line post types, sizes, and spacings to accommodate selected fence heights and fabric sizes for wind loads at various geographical project locations. The *CLFMI Product Manual*, ASTM F1043, and ASTM F1083, as well as the Federal Specification, list the material specifications for the framework.

Chain-Link Fabric

The material specifications for chain-link fabric are thoroughly spelled out in the *CLFMI Product Manual*, ASTM, and Federal Specifications. The choice of chain-link fabric will govern the desired security level, and the various fabric-coating choices will govern the corrosion resistance. Light-gauge residential chain-link fabric will not be considered in this document. Provided are only those chain-link fabrics that offer a level of security, thus the gauge of wire and mesh size has been narrowed down to the following:

11 gauge (0.120 inches diameter)—minimum break strength of 850 lbf

9 gauge (0.148 inches diameter)—minimum break strength of 1,290 lbf

6 gauge (0.192 inches diameter)—minimum break strength of 2,170 lbf

Mesh sizes to consider (mesh size is the minimum clear distance between the wires forming the parallel sides of the mesh) are 2-inch mesh, 1-inch mesh, and $^3/_8$-inch mesh. Consider the following regarding mesh size:

- The smaller the mesh size, the more difficult it is to climb or cut.
- The heavier the gauge wire, the more difficult it is to cut.

The various mesh sizes available in the three previously discussed gauges are listed in the order of their penetration resistance/security:

1. Extremely high security: $^3/_8$-inch mesh 11 gauge
2. Very high security: 1-inch mesh 9 gauge
3. High security: 1-inch mesh 11 gauge
4. Greater security: 2-inch mesh 6 gauge
5. Normal industrial security: 2-inch mesh 9 gauge

Gates

Gates are the only moveable part of a fence and therefore should be properly constructed with appropriate fittings. Chain-link gate specifications are listed in the *CLFMI Product Manual*, ASTM, and Federal Specifications.

Limiting the size of the opening increases vehicular security and reduces the possibility of one vehicle passing another, and the smaller opening reduces the open close cycle time. The cantilever slide gate is the most effective for vehicle security, especially one that is electrically operated and tied into an access control system. High-speed cantilever slide gate operators are available for certain applications.

Pedestrian/personnel gates can be constructed using a basic padlock or designed with an electrical or mechanical lock or a keypad/card key system tied into an access control system. Pre-hung pedestrian gates/portals installed independent of the fence line are available to isolate the gate from fence lines containing sensor systems thus reducing possible false alarms.

DESIGN FEATURES AND CONSIDERATIONS

Some basic design features to consider that enhance security:

- **Height.** The higher the barrier the more difficult and time-consuming it is to broach.
- **Eliminating top rail.** Omission of a rail at the top of the fence eliminates a handhold, thus making the fence more difficult to climb. A 7-gauge coil spring wire can be installed in place of the top rail.
- **Adding barbwire.** Addition of three or six strands at the top of the fence increases the level of difficulty and time to broach. When using the three-strand 45-degree arm it is recommended to angle the arm out from the secured area.
- **Bolt or rivet barbwire arms to post.** Barbwire arms are normally held to the post by the top tension wire or top rail. For added security they can be bolted or riveted to the post.
- **Adding barbed tape.** Stainless steel barbed tape added to the top and in some cases the bottom of the fence greatly increases the difficulty and time to broach.
- **Adding bottom rail.** Addition of a bottom rail that is secured in the center of the two line posts using a 3/8-inch diameter eye hook anchored into a concrete footing basically eliminates the possibility of forcing the mesh up to crawl under the fence. The bottom of the fence, with or without a bottom rail, should be installed no greater than 2 inches above grade.
- **Bury the chain-link fabric.** Burying the fabric 12 inches or more will also eliminate the possibility of forcing the mesh up.
- **Colored chain-link fabric.** One of the security features of a chain-link fence is visibility, allowing one to monitor what is taking place inside or outside of the fence line more efficiently. Color polymer-coated chain-link fabric enhances visibility, especially at night. Complete

polymer-coated systems including coated fabric, fittings, framework, and gates, increase visibility and provide greater corrosion resistance, especially for use in areas adjacent to the seacoast.

- **Double row of security fencing.** It is not uncommon to add an additional line of internal security fencing 10–20 feet inside the perimeter fence. In many cases double rows of fencing are used with sensors and detectors, or with a perimeter patrol road in the area between the fences.
- **Clear zone.** In wooded or high grass areas it is advisable to clear and grub a clear zone on either side of the fence to aid surveillance.
- **Internal security fencing.** Many situations require the need of a separate interior fence to add another level of security for a particular building, piece of equipment, or location.
- **Peen all bolts.** This eliminates the removal of the bolt nut.
- **Addition of a sensor system.** This adds another level of security to the fence system.
- **Addition of lighting.** Increases visibility as well as raises the level of psychological deterrent.
- **Signage.** Installed along the fence line, signs are important to indicate private secured areas (violators may be subject to arrest), and possibly note the presence of alarms and monitoring systems.

TYPICAL DESIGN EXAMPLE

We have chosen for our example to list the referenced specifications separately to help identify the various items that need to be specified. The specification writer may use this format or the standard construction specifications institute (CSI) format in developing their document.

In developing specifications for a typical chain-link fence, the design could be described as follows:

*8′0″ high chain-link fence plus 1′0″, three strands of barbwire at top for a total height of 9′0″, consisting of 2 inches mesh 6-gauge chain-link fabric, *_____ o.d. or *_____ "C" line posts spaced a maximum of 10′0″ o.c., 7-gauge coil spring wire at top, secured to the chain-link fabric with 9-gauge hog rings spaced not greater than 12 inches, $^{15}/_{8}$-inch o.d. bottom rail secured in the center with a $^{3}/_{8}$-inch diameter galvanized steel eye hook anchored into a concrete footing, chain-link fabric secured to line post and rail at a maximum of 12 inches o.c. using 9-gauge tie wire.*

**_____ o.d. end and corner posts complete with $^{15}/_{8}$-inch o.d. brace rail, $^{3}/_{8}$-inch truss assembly, 12-gauge tension bands secured at a maximum of 12-inch o.c., tension bar, necessary, fittings, nuts, and bolts.*

*Chain-link fabric shall comply with ASTM ____.**

*Post and brace rail shall comply with ASTM ____.**

*Barbwire shall comply with ASTM ____.**

*Fittings, ties, nuts, and bolts shall comply with ASTM ____.**

*Coil spring wire shall comply with ASTM ____.**

**Reference is made to ASTM as an example. All chain-link specifications, fabric, posts, fittings gates, and so forth are referenced in ASTM F 1553, Standard Guide for Specifying Chain-Link Fence.*

A typical design/specification for gates would be listed as follows:

*Pedestrian/personnel swing gates shall have a 4′0″ opening by 8′0″ high plus 1′0″, and three strands of barbwire on top. Gate frames shall be fabricated from 2-inch o.d. or 2-inch square members, welded at all corners. Chain-link fabric shall be installed to match the fence line unless otherwise specified. Gateposts shall be *_____ o.d. complete with $1^{5}/_{8}$-inch o.d. brace rail, $^{3}/_{8}$-inch diameter truss assembly, 12-gauge tension bands*

secured a minimum of 12 inches apart, necessary tension bar, fittings, and nuts and bolts.

Chain-link fabric shall comply with ASTM ____.

Swing gates shall comply with ASTM ____.

Gateposts size, o.d., shall comply with ASTM ____.

Gateposts shall comply with ASTM ____.

Fittings shall comply with ASTM ____.

*Cantilever slide gates shall be of the opening sizes as indicated on the drawings, having a height of 8′0″ plus 1′0′, and three strands of barbwire. (The construction and design of cantilever slide gates vary; therefore it is best to list the specific specification.) Cantilever slide gates shall be constructed per ASTM F 1184, Class *____. Chain-link fabric shall match the fence line unless otherwise specified. (Cantilever slide gates require 4-inch o.d. gateposts; larger or smaller posts are not recommended.) The 4-inch o.d. gateposts shall be complete with $1\frac{5}{8}$-inch o.d. brace rail, $\frac{3}{8}$-inch diameter truss assembly, 12-gauge tension bands secured a minimum of 12 inches apart, necessary tension bar, fittings, and nuts and bolts.*

4-inch o.d. gatepost and $1\frac{5}{8}$-inch o.d brace rail shall comply with ASTM ____.

Fittings shall comply with ASTM ____.

Chain-link fabric shall comply with ASTM ____.

Installation

Installation for the fence line, terminal posts, and gates varies depending on the security level required, site conditions, geographical location, and soil and weather conditions. The best documents to assist you in this process are ASTM F 567, "Standard Practice for Installation of Chain-Link Fence," and the CLFMI "Wind Load Guide for the Selection of Line Post Spacing and Size."

Project Inspection

Improper material or installation can have a dramatic effect on the required security. It is important to verify that the project materials are in compliance with the contract specifications and that the fence has been installed properly. Procurement or facility managers may want to consider a mandatory requirement of their reviewing material certifications and shop drawings prior to the start of the project. This will ensure that proper products will be installed and that specific installation guidelines have been provided. CLFMI offers a *Field Inspection Guide* document to assist in this process.

Reference is made to various fence specifications; complete information can be obtained by contacting the following:

Chain-Link Manufacturers Institute 10015 Old Columbia Road, Suite B-215, Columbia, MD 21046; Phone: 301-596-2583; http://www.chainlinkinfo.org/

Standardization Documents Order Desk Federal Specification RR-191K/GEN Bldg. 4D, Robbins Ave., Philadelphia, PA 19120-5094

ASTM 100 Barr Harbor Drive West, Conshohocken, PA, 19428; Phone: 610-832-9500; http://www.astm.org/

Construction Specifications Institute 99 Canal Center Plaza, Suite 300, Alexandria, VA 22314; Phone: 800-689-2900; emembcustsrv@csinet.org

In addition to information available from the above-listed organizations, design and engineering assistance is available through a number of CLFMI member firms. To find these firms, click on "Product/Services Locator" and select "All United States" and "Security Chain-Link Fence Systems" from the product listing. Then click "GO" and the firms who can assist you will be listed.

FIGURE 14-1

FIGURE 14-2

FIGURE 14-3

FIGURE 14-4

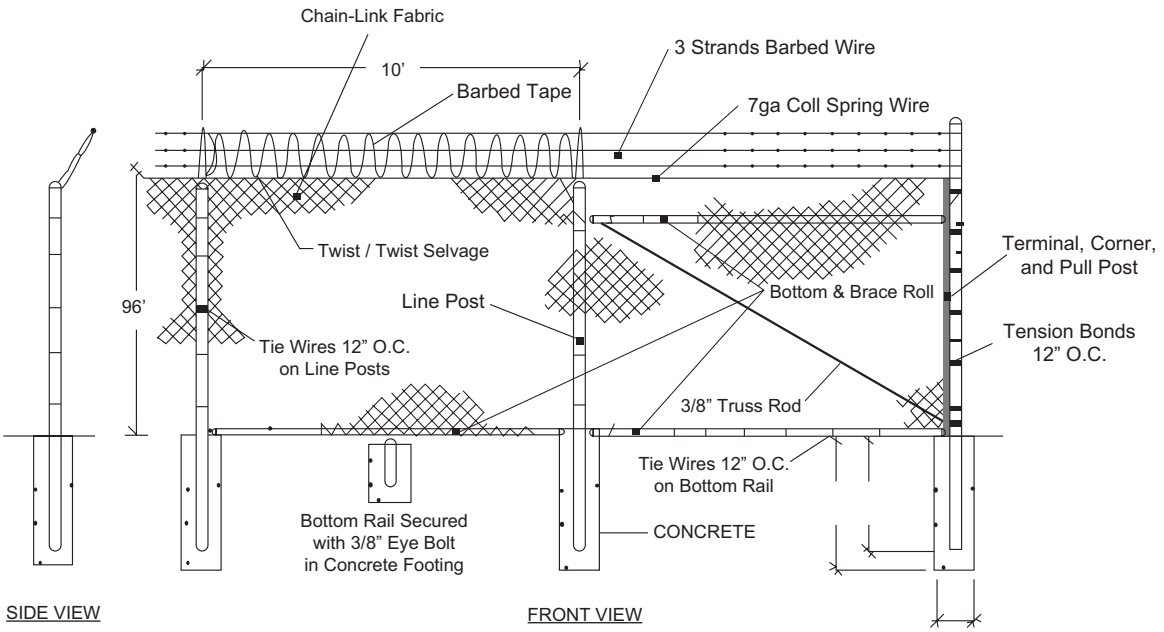


FIGURE 14-5 Typical detail of an 8-foot-high fence with 1-foot, three-strand barbed wire security.

CHAPTER

15

Stages of Fire

Inge Sebyan Black, CPP

STAGES OF FIRE

1. **Ignition.** Fuel, oxygen and heat join together in a sustained chemical reaction. At this stage, a fire extinguisher can control the fire.
2. **Growth.** With the initial flame as a heat source, additional fuel ignites. Convection and radiation ignite more surfaces. The size of the fire increases and the plume reaches the ceiling. Hot gases collecting at the ceiling transfer heat, allowing all fuels in a room to come closer to their ignition temperature at the same time.
3. **Fully developed.** Fire has spread over much if not all the available fuel; temperatures reach their peak, resulting in heat damage. Oxygen is consumed rapidly.
4. **Decay (burnout).** The fire consumes available fuel, temperatures decrease, and the fire gets less intense.

HOW FIRE SPREADS

Fire spreads by transferring the heat energy from the flames in three different ways.

- **Conduction.** The passage of heat energy through or within a material because of direct contact, such as a burning wastebasket heating a nearby couch, which ignites and heats the drapes hanging behind, until they too burst into flames.
- **Convection.** The flow of fluid or gas from hot areas to cooler areas. The heated air is less dense and rises, while cooler air descends. A large fire in an open area produces a plume or column of hot gas and smoke high into the air. But inside a room, those rising gases encounter the ceiling. They travel horizontally along the ceiling forming a thick layer of heated air, which then moves downward.
- **Radiation.** Heat traveling via electromagnetic waves, without objects or gases carrying it along. Radiated heat goes out in all directions, unnoticed until it strikes an object. Burning buildings can radiate heat to surrounding structures, sometimes even passing through glass windows and igniting objects inside.

FOUR WAYS TO PUT OUT A FIRE

1. Cool the burning material.
2. Exclude oxygen.
3. Remove the fuel.
4. Break the chemical reaction.

CLASSIFYING FIRE

Fire classifications based on fuel type:

Class A. Ordinary combustible materials, such as wood, cloth, paper, rubber, and many plastics. They burn with an ember and leave an ash. Extinguish by cooling the fuel to a

temperature that is below the ignition temp. Water and other extinguishing agents are effective.

Class B. Flammable liquids (burn at room temperature) and combustible liquids (require heat to ignite). Petroleum greases, tars, oils, oil-based paints, solvents, lacquers, alcohols, and flammable gases. High fire hazard; water may not extinguish. Extinguish by creating a barrier between the fuel and the oxygen, such as layer of foam.

Class C. Fuels that would be A or B except that they involve energized electrical equipment. Special techniques and agents required to extinguish, most commonly carbon dioxide or dry chemical agents. Use of water is very dangerous because water conducts electricity.

Class D. Combustible metals, such as magnesium, titanium, zirconium, sodium, lithium, and potassium. Most cars contain numerous such metals. Because of extremely high flame temperatures, water can break down into hydrogen and oxygen, enhancing burning or exploding. Extinguish with special powders based on sodium chloride or other salts; also clean dry sand.

Class K. Fires in cooking appliances that involve combustible cooking media (vegetable or animal oils and fats).

UL STANDARD 217

UL Standard 217, "Single and Multiple Station Smoke Alarms," allows for dual-sensor alarms so long as each sensor is primarily a smoke sensor and the design meets the standard. The alarm logic is an {OR}-type such that the alarm is activated if either the photoelectric sensor or ionization sensor alarm threshold is met. The individual sensor sensitivities are not tested separately. Therefore, manufacturers have the freedom to set each sensor's sensitivity separately. Since an individual sensor can be set to meet all current sensitivity standards, it is not obvious what overall benefit is achieved from a dual alarm with an additional sensor technology that could be more or less sensitive than what would be found in a standalone unit employing such a sensor. Additionally, another potential benefit of a dual-sensor alarm may be realized by adjusting each sensor's alarm threshold to reduce nuisance alarms. Thus, the sensitivity of each sensor factors into the overall performance of a dual alarm.

Table 15.1 shows the distributions of ionization, photoelectric, and dual alarm times in histograms with the median and mean alarm times indicated. These particular distributions arise in part from the variation of the fire sources and locations of the alarms.

Since individual sensor sensitivities were not known, an estimate of which ionization and photoelectric sensor was more sensitive was made (either the ionization alarm or the ionization sensor in the dual alarm, and either the photoelectric alarm or the photoelectric sensor in the dual alarm). To make this judgment, the following logic was considered. Between the ionization and photoelectric alarm, the ionization alarm was the first to respond in 18 of the 54 instances, responding 83 sec faster on average than the photoelectric alarms. Considering those 18 instances, the dual alarm responded first in 17 of those instances, and responded 81 sec faster on average than the ionization alarm (SD = 158 sec), with a median response 19 sec faster. In addition to the above detectors, there are also Obscuration Detectors which due to smoke, light is decreased, Thermal Detectors used in the detection of *predetermined* temperature, and

TABLE 15.1 Average Alarm Times for NRC Canada Test Series

Alarm Type	Average Alarm Time (sec)	Standard Deviation (SD) (sec)
Ionization alarm	1,205	1,102
Photoelectric alarm	666	537
Dual alarm	587	450

Note: All were initially smoldering fires.

Infrared Flame Detectors, in which the emission from the flame trips the infrared [2].

WATER SUPPLY FOR SPRINKLERS AND TANKS [3]

For automatic sprinklers to operate, there must be a supply of water to the sprinkler that opens to extinguish or control fire and prevent it from spreading. This water may come from a variety of sources such as public water systems, usually considered the principal or primary water supply, and storage tanks of different types (see NFPA 13, Standard for the installation of Sprinkler Systems).

Gravity tanks are tower or roof mounted and are used in high-rise buildings. Suction tanks are equipped with automatically operated fire pump(s), pressure tanks are pressurized water reservoirs used to supply a limited amount of water, and a fire pump (some fire pumps are called booster pumps because they boost the pressure) is a mechanical device for improving the water supply pressure.

The types of automatic sprinkler systems are as follows:

- Wet-pipe systems
- Dry-pipe systems
- Preaction systems

The types of stand pipe systems are as follows:

- Automatic-wet systems
- Automatic-dry systems
- Semiautomatic-dry systems

The automatic-wet stand pipe system is most commonly installed in modern high-rise buildings with a fixed water supply not exposed to freezing.

REFERENCES

[1] NFPA website, www.nfpa.org
[2] Presented at the Fire Protection Research Foundation's 13th Annual Suppression and Detection Research and Applications Symposium (SUPDET 2009), February 24–27, 2009, Orlando, FL.
[3] Craighead G. High-rise security and fire life safety. 3rd ed.; 2009 Waltham, MA.

APPENDIX 16.A. FIRE SAFETY INSPECTION

Michael Sroberger

The following inspection is designed to be the basis of a revised and property-specific inspection program. Some of the entries refer to functions performed with a "reasonable frequency." In reviewing your specific property or location, care should be taken to consider the nature of the structure, geographic location, intended use, and actual use. In many cases, functions that are best performed on a daily basis in one environment can be reasonably performed on a weekly or possibly monthly basis in a different environment.

In addition, note that every application is unique in some manner. As such, what might be prudent for one location, however seemingly similar, might be insufficient at another location. While benchmarking of a similar program is highly recommended, this also should be seen as simply a basic guideline in the creation of a customized, location-specific program.

Some sections pose inspection inquiries that reference a large number of possible locations or items to be reviewed. One example would be the inspection of sprinkler heads. In designing the actual checklist for such an inspection, it is often desirable to break down the physical layout of the facility into reasonable and manageable zones. Identifying sets of sprinkler heads by the room in which they are installed allows the person performing the inspection to review them as a set and make comments in reference to that area of coverage. In cases such as fire doors, it might be reasonable to identify them with a location number, which could be included not only on the inspection form, but a numbered tag, on the hinge-side edge of the door, for later identification.

ADMINISTRATIVE AND PLANNING PHASE

- Are copies of all locally enforced codes maintained on site for reference?
- Does the facility meet requirements of locally enforced building code?

- Does the facility meet requirements of locally enforced fire prevention code?
- Does the facility meet requirements of locally enforced life safety code?
- Does the facility have a written and appropriately distributed Fire Prevention and Response Plan? Is this plan known to all employees? Is training provided to those with defined responsibilities? Is all training documented and securely filed? Is the plan reviewed annually, updated as required, and redistributed?
- Does the facility maintain a fire brigade? Is the fire brigade training documented and securely filed? Is the fire brigade training conducted in conjunction with the local fire department? Is the fire brigade comprised of persons, or positions, that are present or represented at all times?
- Are all inspection reports retained for a reasonable number of years, as defined by local codes, insurance requirements, or industry standards? Are inspection reports filed in a secure location?
- Are all employees trained in basic fire prevention concepts and fire event response procedures? Is the content of this training consistent and reasonably inclusive? Is this training documented and securely filed? Is annual refresher training conducted? Is annual refresher training documented and securely filed?

GENERAL PHYSICAL INSPECTION PHASE

- Are all fire exit routes clearly marked? Are all exit routes unobstructed at all times? Are all exit routes and egress hardware items in compliance with the Americans with Disabilities Act (ADA) requirements?
- Are all fire doors and egress hardware items in proper working order?
- Are service areas secured against unauthorized entry when not in use?
- Are all areas free of loose or disorganized combustible items (such as rags or empty boxes)?
- Are all storage areas well organized, to allow ease of access in emergency situations?
- Are flammable or combustible items properly stored to protect against accidental ignition?
- Are flammable or combustible items properly stored to protect against unauthorized usage or tampering?
- Are all fire lanes clearly marked? Are fire lanes maintained in an unobstructed condition at all times?
- Are master keys available for fire department use at all times?
- Are all electrical panels accessible at all times? Are all panels clearly marked, to facilitate emergency power disconnection?
- Are gas line shutoff valves accessible at all times?
- Are all gas-operated pieces of equipment inspected for wear and damage with reasonable frequency? Are inspections documented and filed in a secure location?
- Are all heat-generating devices (such as boilers, furnaces, and dryers) provided a reasonable clear zone, based on levels of heat output, where storage of any kind is prohibited?
- Are all ducts inspected regularly and cleaned as required?
- Is the use of extension cords discouraged in all areas?
- Are all electrical cords and electrically operated items inspected for wear or damage with reasonable frequency? Are such inspections documented?
- Are designated smoking areas clearly defined and at a proper minimum safe distance from any common or identified ignition threats? Are appropriate ash and cigarette receptacles available for use in these areas? Are they per state laws?

EXTINGUISHER INSPECTION PHASE

- Have all extinguishers been inspected and serviced as required by a licensed vendor or trained technician within the past 12 months?
- Are all extinguishers of a type appropriate for most probable types of fires in the immediate area?

- Are specialty extinguishers available in those areas that would require them?
- Are persons trained in the use of the extinguishers available in the areas where they are typically present? Is this training documented and filed in a secure location?
- Are extinguishers inspected with reasonable frequency (daily, in most cases), to ensure that they are present and have not been tempered with or discharged? Is each extinguisher inspection fully documented and securely filed?

STAND PIPE, FIRE HOSE, AND CONTROL VALVE INSPECTION PHASE

- Do tamper switches, linked to an alarm system, monitor all control valves?
- Are all control valves inspected and tested annually by a licensed vendor or trained technician?
- Are all stand pipes, control valves, and fire hoses accessible at all times?
- Are fire hoses inspected, per manufacturer recommendations, for wear and decay?

SPRINKLER SYSTEM INSPECTION PHASE

- Are all flow switches inspected and tested annually by a licensed vendor or trained technician?
- Are all sprinkler heads of a type appropriate for the location in which they are installed?
- Are all sprinkler heads installed and maintained within the manufacturers' recommendations?
- Are all sprinkler heads provided with a clear area of operation, in compliance with local fire codes?
- Does the sprinkler system have a pressure maintenance pump? If so, is this pump inspected and tested with reasonable frequency (weekly, in most cases) by a licensed vendor or trained technician?
- Are all areas requiring sprinkler system coverage, per the local fire code, provided with such coverage?

HAZARDOUS MATERIALS INSPECTION PHASE

- Are proper warning placards utilized in areas of chemical storage and usage?
- Is proper personal protective equipment (PPE) provided for initial response to fire and emergency situations related to any hazardous materials that are maintained or utilized on site? Is training provided in the use of this PPE? Is such training documented and filed in a secure location?
- Is the fire department made aware of storage areas, use areas, and large arriving or departing shipments of hazardous materials?
- Are all appropriate containment, standoff distance, and warning signals utilized in storage areas?
- Are MSDS books on file and accessible 24/7?

ALARM SYSTEM INSPECTION PHASE

- Is the system monitored by a licensed, off-site monitoring service?
- Is the system inspected and tested annually by a licensed vendor or trained technician?
- Is this inspection documented and filed in a secure location?
- Is the area of coverage broken down into identified zones?
- When activated, does the alarm system clearly identify the location of the potential fire?
- Are audible alarms heard in all areas of a zone when activated? Is the system designed to warn adjacent zones, inclusive of floors above or below?
- Are strobes visible in all areas of a zone when activated? Is the system designed to warn adjacent zones, inclusive of floors above or below? Are there any ADA complaints?
- Does the alarm system record activation and use history? For what length of time is this history retained?
- Does the system's audible signal include a prerecorded advisory message? If so, does this message recommend a route or method of egress?

If so, does this message advise against the use of elevators if any are present?
- Does the system automatically recall or drop elevators on activation? Are override keys available for fire department use?
- Are detector types installed as appropriate for the specific location of installation? If the intended use of a given area is altered, is the type of detector also reviewed and changed to match the updated intended use of that area?

CHAPTER

16

Standards, Regulations, and Guidelines: Compliance and Your Security Program, Including Global Resources

Roderick Draper

INTRODUCTION

While the nature of the risks to which organizations are exposed vary widely, the need to have a clearly defined and defensible approach to risk management is common to all private and public sector enterprises. But where do you start?

Some industries are heavily regulated in the areas of physical and information security and the regulations provide direction for those responsible for risk management. For example, the Nuclear Regulatory Commission is responsible for defining and enforcing compliance with security requirements at commercially operated nuclear power stations in the United States and as part of its mandate publishes a range of guidelines to support regulatory compliance. Similarly, but on a very different scale, workplace health and safety regulations in Queensland, Australia, require employers within the retail industry to develop risk management strategies relating to the threat of robbery. To assist organizations with managing their robbery-related risks and associated regulatory compliance, the Department of Industrial Relations publishes a guide that includes a range of strategies.

Notwithstanding the context within which a security program may exist, the strategies for understanding and managing security-related risks can be divided into two core groups:

1. Mandatory practices
2. Benchmark (minimum) practices

Mandatory practices are essential to meet legislative, regulatory, licensing, registration, or similar compliance requirements. These may be applicable to the activities in which the enterprise is engaged and/or be specific to risk management programs. For example, Bill 168 in Ontario, Canada, amended the Occupational Health and Safety Act (OHSA) to incorporate strict new standards in an attempt to reduce violence and harassment in the workplace. These requirements apply to all workplaces with five employees or more, and the Ministry of Labour has published guidelines to assist organizations with understanding the requirements and implementing appropriate strategies. Similarly, in-house security officers in

some jurisdictions are required to receive specified training and hold licenses issued by a local regulatory authority. Any organization operating within such a jurisdiction must incorporate into its security program all practices necessary to ensure compliance with the security licensing requirements.

Benchmark (minimum) practices are those approaches that in legal terms could "reasonably" be expected to be followed, given the specific circumstances that apply. For example, standards such as ISO 31010:2009, "Risk Management—Risk Assessment Techniques," provide generic guidance with respect to assessing a wide range of risks, but compliance with the process described in the standard is not necessarily mandatory. Strategies defined in standards published by recognized standards bodies only become mandatory where those standards are specified for compliance (e.g., electrical wiring standards specified in electrical safety regulations). However, where a published standard or guideline has clear application in the management of security-related risks, it should be carefully considered by the enterprise as a potential benchmark to be followed. Such recognized standards and guidelines provide a defensible basis for security management decisions. Taken in context, they can be used to support a business case for security expenditure or support a policy position.

Implementation of strategies can, of course, depart from those described in nonmandatory standards and guidelines; however, such decisions need to be made in an informed manner so that they are clearly supported by all the factors that should be considered. If decisions are made not to follow published standards and guidelines that are applicable to the management of security-related risks within the enterprise, it is important to reflect on how defensible those decisions would be in litigation or under scrutiny by the media or an aggrieved party to a risk event.

For example, there was a decision of the Supreme Court of Victoria, Australia, in 2009 relating to a robbery that occurred at a hotel (*Ogden v. Bell Hotel Pty Ltd.* [2009] VSC 219). The court held that the hotel's failure to implement reasonable security measures had contributed and led to the opportunity for the robbery. Although the hotel tried to argue that they had informal measures and expectations relating to security, they simply did not have a structured and defensible approach to security risk management. The hotel's failure to properly consider all of the risks and ensure that policies and procedures were developed in accordance with reasonable and expected practices contributed to the plaintiff being awarded $825,000 in damages.

STANDARDS

In this context the term *standard* means a document published by a recognized standards body for the purpose of specifying requirements and/or an approach to a specific subject area. There are literally hundreds of recognized standards bodies around the world operating within geographic or industry/technology boundaries. At an international level, there are numerous organizations that develop and publish standards for universal consumption. One of the largest is the International Organization for Standardization (ISO; *www.iso.org*).

In recent years the ISO has published a number of standards that have been derived from those published by national standards bodies. Subsequently, these new ISO standards have been adopted by the countries concerned in favor of or in addition to the originating local standard. For example, the Canadian Standards Association (CSA; *www.csa.ca*) developed and published its standard CAN/CSA-Q850-97, "Risk Management: Guideline for Decision Makers," in 1997. While Q850 remains a current Canadian standard, in 2010 CSA also adopted the ISO standard ISO 31000:2009, "Risk Management—Principles and Guidelines," and now publishes this under the title CAN/CSA-ISO 31000-10, "Risk Management—Principles and Guidelines." Similarly, the Australian and New Zealand standards bodies had initially published their risk

management standard in 1995 and revised it several times until it was last published in 2004. When the ISO standard was published in 2009, it was adopted for use in Australia and New Zealand under the title AS/NZS ISO 31000:2009, "Risk Management—Principles and Guidelines." Unlike Q850 in the Canadian context where the original standard remains valid, the local standard (AS/NZS 4360) was superseded by the international standard (AS/NZS ISO 31000).

It is important to note that while not all ISO standards are adopted by regional or national standards bodies, they may still have application for security programs within those geographic locations. For example, the ISO standard for risk assessment mentioned in the introduction to this chapter has been widely adopted by standards bodies including the CSA, Asociación Española de Normalización y Certificación (AENOR; *www.aenor.es*), European Committee for Electrotechnical Standardization (CENELEC; *www.cenelec.eu*), Association française de normalisation (AFNOR; *www.afnor.org*), British Standards Institution (BSI; *www.bsigroup.com*), and Österreichisches Normungsinstitut (ON, Austrian Standards Institute; *www.as-institute.at*), just to name a few. In contrast, the ISO risk management standard has not been embraced by the Australian and New Zealand standards bodies that adopted the ISO 31000 standard.

The application of any published standard must be considered in context with the benefits that will be derived through its adoption. While mandated regulatory requirements may be more likely to be drawn from national or international standards, those developed and published by industry bodies tend to be more specific in nature and underpin benchmark or minimum accepted practices. Apart from traditional participation on standard development committees, a number of recognized industry associations have developed working relationships with standards bodies to jointly develop and publish standards and guidelines. For example, ASIS International (*www.asisonline.org*) worked with the BSI to develop the standard ASIS/BSI BCM.01-2010, "Business Continuity Management Systems: Requirements with Guidance for Use." This joint industry/national standard is based on a BSI standard that is adapted for consideration within the security risk management context. Similarly, BSI has partnered with the Institute of Electrical and Electronics Engineers (IEEE; *www.ieee.org*) in the development of joint standards, and the North American Security Products Organization (NASPO) collaborated with the American National Standards Institute (ANSI; *www.ansi.org*) to produce ANSI/NASPO-SA-2008, "Security Assurance Standards for the Document and Product Security Industries."

The range of national, international, and industry standards that may be applicable to the management of individual security programs is far too extensive and dynamic to be listed in a volume such as this. It is important to consider standards covering both mandatory and benchmark practices, including those developed and published by national standards bodies and industry organizations. Where there are no locally applicable standards within a particular area of the security program, it is worthwhile reviewing those that may apply within other jurisdictions. Ultimately, and notwithstanding regulatory obligations, the application of provisions within a standard can be used to provide a structured approach to a given issue, deliver defensibility for decisions, and establish consistency across a security program.

REGULATIONS

Almost universally, all security programs must consider regulatory compliance with respect to workplace safety and life safety. However, there are many other areas where legislative, regulatory, licensing, registration, or similar compliance requirements are met through, or have a direct impact on, the security program. For example, the use of closed-circuit television (CCTV) as a security strategy is widespread. But deploying and operating a camera within any given space may come with a number of compliance requirements that may not be applicable in another

location. Some of the regulatory considerations for deploying a CCTV camera might include:

- Licensing of the installer (e.g., as required in the Canadian Province of British Columbia; *www.pssg.gov.bc.ca*).
- Licensing of the camera operator (e.g., as required in the United Kingdom; *www.sia.homeoffice.gov.uk*).
- Conditions for installation (e.g., as required in workplaces in the Australian State of New South Wales; *http://www.austlii.edu.au/au/legis/nsw/consol_act/wsa2005245/s11.html*).
- Registration of the CCTV system (e.g., as in Western Australia; *https://blueiris.police.wa.gov.au/*).
- Training for operators (e.g., as nominated in the Australian capital territory for bus cameras; *http://www.tams.act.gov.au*).
- Privacy management (e.g., in line with the Privacy Act in New Zealand; *www.privacy.org.nz*, and Standards for the Protection of Personal Information in Massachusetts; *http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf*).
- Documentation (e.g., in accordance with the requirements of the Commission d'accès à l'information du Québec, Canada; *http://www.cai.gouv.qc.ca/06_documentation/01_pdf/new_rules_2004.pdf*).

Notwithstanding specific laws with respect to firearms, the private security industry worldwide is impacted by escalations in regulatory obligations as authorities come under pressure to address community concerns about the training, competence, and suitability of security personnel to perform their assigned duties. In some jurisdictions licensing and training requirements are only imposed on security contractors and do not apply to in-house security personnel (i.e., those employed directly by the company whose assets they are protecting). Whereas in other regulatory settings, licensing and training obligations are applied equally to in-house and contracted personnel.

In a situation where in-house staff are not legally required to be licensed, an organization may wish to consider the benefits of employing licensed personnel. While there are clearly cost implications in meeting the licensing requirements, the decision to do so may mitigate risks associated with the actions or inactions of security personnel. For example, obtaining and maintaining a security-related license in most jurisdictions incorporates criminal background checks and basic training requirements. In effect, the regulator provides a foundational level of assurance with respect to the license holder's suitability to perform the functions for which he or she is licensed.

History has shown that holding a security industry license does not guarantee that security personnel will act appropriately and lawfully in performing their duties. It does, however, provide a level of defensibility for the decision to deploy a person in a role for which the industry regulator deems him or her to be suitable. This must, of course, be reinforced with robust policies, procedures, standing orders, training, and awareness strategies to ensure that security personnel are made aware of and accept their roles and responsibilities.

While the title of this chapter has the security program as its focus, security-related risks should not be considered in isolation and a holistic approach to risk management is critical to avoiding the pitfalls associated with management "silos." Regulatory compliance can, in fact, be the catalyst for greater cooperation across lines of demarcation that might otherwise be a hindrance to the effective management of specified risks.

As noted in the introduction to this chapter, some industries are heavily regulated in the areas of physical and information security. There are lessons that can be learned by studying the requirements imposed on those industries within the context of your own operations. Regulations are generally implemented to protect the community from identified risks. By judiciously drawing motivation from regulatory controls in related fields, a security program can be significantly enhanced and made far more defensible from litigious actions.

GUIDELINES

While there are a range of published guidelines available to support the implementation of aspects of security programs within specific settings, there are many more that have been developed and remain largely unknown or inaccessible. In the context of this chapter, the term *guidelines* should be taken to include other types of publications with similar purposes, such as manuals, specifications, protocols, practices, templates, aide memoirs, checklists, and fact sheets.

The Federal Emergency Management Agency within the U.S. Department of Homeland Security (FEMA; *www.fema.gov*) publishes guidelines covering many aspects of physical security. Some of the more popular FEMA resources include:

- FEMA 426, "Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings"
  This manual provides guidance to the building science community of architects and engineers, to reduce physical damage to buildings, related infrastructure, and people caused by terrorist assaults. The manual presents incremental approaches that can be implemented over time to decrease the vulnerability of buildings to terrorist threats. Many of the recommendations can be implemented quickly and cost effectively. (*http://www.fema.gov/library/viewRecord.do?id=1559*)
- FEMA 452, "A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings"
  This how-to guide outlines methods for identifying the critical assets and functions within buildings, determining the threats to those assets, and assessing the vulnerabilities associated with those threats. The methods presented provide a means to assess risks and to make decisions about how to mitigate them. The scope of the methods includes reducing physical damage to structural and nonstructural components of buildings and related infrastructure, and reducing resultant casualties during conventional bomb attacks, as well as attacks involving chemical, biological, and radiological (CBR) agents. (*http://www.fema.gov/library/viewRecord.do?id=1938*)
- E155 and L156, "Building Design for Homeland Security"
  The purpose of E155 and L156 is to familiarize students with assessment methodologies available to identify the relative risk level for various threats, including explosive blast and chemical, biological, or radiological agents. Students are introduced to publications FEMA 426 and FEMA 452 and are asked to provide mitigation measures for a range of human-made hazards. The primary target audience for these courses includes engineers, architects, and building officials. (*http://www.fema.gov/library/viewRecord.do?id=1939*)
- FEMA 453, "Safe Rooms and Shelters—Protecting People Against Terrorist Attacks"
  The objective of this manual is to provide guidance for engineers, architects, building officials, and property owners to design shelters and safe rooms in buildings. This manual presents information about the design and construction of shelters in the workplace, home, or community building that will provide protection in response to human-made hazards. (*http://www.fema.gov/library/viewRecord.do?id=1910*)
- FEMA 389, "Communicating with Owners and Managers of New Buildings on Earthquake Risk"
  FEMA 389 was developed to facilitate the process of educating building owners and managers about seismic risk management tools that can be effectively and economically employed during the building development phase—from site selection through design and construction—as well as the operational phase. The document provides guidance for identifying and assessing earthquake-related hazards during the site selection process, including the potential seismic hazards of ground shaking, surface fault rupture, soil liquefaction, soil differential compaction, landsliding, and inundation, as well as other potential hazards affecting building performance, vulnerable transportation, and utility systems (lifelines); the hazards posed by adjacent

structures; the release of hazardous materials; and post-earthquake fires. (*http://www.fema.gov/library/viewRecord.do?id=1431*)

- FEMA 430, "Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks"
  FEMA 430 provides information and design concepts for the protection of buildings and occupants, from site perimeters to the faces of buildings. The intended audience includes the design community of architects, landscape architects, engineers and other consultants working for private institutions, building owners and managers, and state and local government officials concerned with site planning and design. FEMA 430 is one of a series that addresses security issues in high-population private-sector buildings. It is a companion to FEMA 426, which provides an understanding of the assessment of threats, hazards, vulnerability, and risk, and the design methods needed to improve protection of new and existing buildings and the people occupying them. (*http://www.fema.gov/library/viewRecord.do?id=3135*)
- FEMA 427, "Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks"
  This primer introduces a series of concepts that can help building designers, owners, and state and local governments mitigate the threat of hazards resulting from terrorist attacks on new buildings. FEMA 427 specifically addresses four high-population, private-sector building types: commercial office, retail, multifamily residential, and light industrial. This manual contains extensive qualitative design guidance for limiting or mitigating the effects of terrorist attacks, focusing primarily on explosions, but also addressing chemical, biological, and radiological attacks. (*http://www.fema.gov/library/viewRecord.do?id=1560*)
- FEMA 428, "Primer for Design Safe Schools Projects in Case of Terrorist Attacks"
  The purpose of this primer is to provide the design community and school administrators with the basic principles and techniques to design a school safe from terrorist attacks. (*http://www.fema.gov/library/viewRecord.do?&id=1561*)

Industry associations are an excellent source for guidelines to support security programs. For example, ASIS International develops and publishes a range of guidelines that are available free of charge to its members and that may be purchased by nonmembers. Some of the subjects covered include (*http://www.asisonline.org/guidelines/published.htm*):

- Business continuity
- Facilities physical security measures
- General security risk assessment
- Information asset protection
- Pre-employment background screening
- Private security officer selection and training
- Threat advisory system response
- Workplace violence prevention

The American Public Transportation Association also publishes a number of security-related guidelines, including:

- APTA SS-SEM-RP-001-08, "Recommended Practice for a Continuity of Operations Plan"
- APTA SS-SEM-RP-002-08, "Recommended Practice for First Responder Familiarization of Transit Systems"
- APTA SS-SEM-RP-003-08, "Recommended Practice: Security and Emergency Management Aspects of Special Event Service"
- APTA SS-SEM-RP-004-09, "Recommended Practice: General Guidance on Transit Incident Drills and Exercises"
- APTA SS-SEM-RP-005-09, "Recommended Practice: Developing a Contagious Virus Response Plan"
- APTA SEM-SS-RP-008-09, "Recommended Practice: Safe Mail and Package Handling"
- APTA SEM-SS-RP-009-09, "Recommended Practice: Emergency Communication Strategies for Transit Agencies"
- APTA SS-SEM-RP-012-09, "Recommended Practice: Responding to Threat Condition Levels"

- APTA SS-SIS-RP-002-08, "Recommended Practice for CCTV Camera Coverage and Field of View Criteria for Passenger Facilities"
- APTA RP-CCS-1-RT-001-10, "Securing Control and Communications Systems in Transit Environments, Part 1"

Care needs to be taken when reviewing guidelines for potential use in any given application to ensure that they do not conflict with any regulations or published standards that may be applicable. For example, the process for assessing security-related risks as defined in the ISO 31010 standard differs significantly from the "ASIS General Security Risk Assessment Guideline" described earlier. While each situation will need to be evaluated in the relevant contexts, as a general rule the following hierarchy of authority can be used as a guide:

1. Legislation/regulations
2. Standards (by recognized standards body)
3. Guidelines

Regulators also routinely publish guidelines to assist organizations with compliance, and it is important to recognize that where such guidelines exist, they should be considered as a foundation for the applicable areas of the security program. Guidelines themselves do not in most cases have any statutory standing but may be referenced in separate regulatory instruments.

For example, the government of the State of Queensland in Australia has published crime prevention through environmental design guidelines (CPTED; *http://www.police.qld.gov.au/programs/cscp/safetyPublic/*). The Queensland CPTED guidelines are referenced by local governments in their policies and by-laws, establishing a pseudo regulatory role for the guidelines in this example. The CPTED guidelines are specifically mandated as a policy within the Southeast Queensland Regional Plan 2009-2031 and the associated regulatory provisions (see Policy 6.3.4, p. 80). By referencing the CPTED guidelines in planning scheme policy, new developments can be assessed for compliance against practices nominated in the guidelines. Where deviations from the approaches described in the CPTED guidelines are identified, developers can be required to make the changes necessary for compliance.

Many guidelines developed by government agencies are not linked to regulatory requirements but still bear consideration when developing elements of a security program. For example, the "National Code of Practice for CCTV Systems for the Mass Passenger Transport Sector for Counterterrorism" includes recommendations for operational objectives and minimum storage requirements, but these have not been adopted as widely as the authors may have wished because of the cost of compliance. In the absence of regulatory compliance obligations or other compelling business risk, the guidelines in this case are little more than informative (*http://www.coag.gov.au/coag_meeting_outcomes/2006-07-14/docs/cctv_code_practice.rtf*).

Standards bodies may develop guidelines as complementary documents to published standards. The *Australian Standards Handbook*, HB 167:2006, "Security Risk Management," outlines "a broad framework and the core elements that should be included in a security risk management process, and is consistent with the risk management principles of AS/NZS 4360: 2004" (*https://infostore.saiglobal.com/store/details.aspx?ProductID=568733*). This handbook is in turn referenced in the "Risk Management Kit for Terrorism" published by the Department of Transport in the Australian state of Victoria, which is "designed to assist operators of declared essential services (DES) to meet their legislative requirements under the Terrorism (Community Protection) Act 2003." This interweaving of statutory obligations, standards, and guidelines demands careful consideration and detailed review in managing compliance within the operational contexts that apply.

MANAGING COMPLIANCE

Every organization, regardless of size or sector of operations, can benefit from having a structured security management plan. The plan does not necessarily need to be complex, but it does need to recognize the range of risks to which the

organization is exposed, including specific compliance-related risks. Inherently, the governance framework that overlays the security program needs to include mechanisms for monitoring compliance obligations and prioritizing decisions in relation to the management of related risks.

For example, the Sarbanes-Oxley Act 2002 (SOX), which is administered by the U.S. Securities and Exchange Commission, has significant implications for physical and information security programs. Managing SOX compliance requires a clear understanding of the range of risks that may lead to adverse audit outcomes and associated penalties. Given that records need to be retained for not less than five years, the SOX compliance element of the security program must take into account the full range of strategies necessary to prevent the records from compromise through:

- Loss or destruction
- Denial of access
- Unauthorized modification or alteration
- Contamination

The SOX legislation does not dictate how records are to be protected; it simply defines the outcome required. To some extent this opens up a wide range of options for risk management but does not offer any guidance to support compliance management.

In contrast, some government agencies publish an extensive range of resources to support managing compliance with policy and regulatory obligations. For example, the "Australian Government Protective Security Policy Framework" is the means through which agencies are to achieve the mandatory requirements for protective security expected by government. To facilitate compliance management processes, a range of supporting documents are provided, including:

- "Protective Security Guidance for Executives"
- "Security Awareness Training Guidelines"
- "Australian Government Personnel Security Protocol"
- "Agency Personnel Security Guidelines"
- "Security Clearance Subjects Guidelines"
- "Procedural Fairness Guidelines"
- "Reporting Changes in Personal Circumstances Guidelines"
- "Contact Reporting Guidelines"
- "Personnel Security Practitioners Guidelines"
- "Personnel Security Adjudicative Guidelines"

Ultimately, compliance management requires a structured approach to understanding obligations and risks, and facilitates defensible decisions based on a clear understanding of the implications for noncompliance in the context within which operational risks exist. While guidance may be available for some regulatory and policy compliance obligations, those responsible for managing security-related risks should ensure that all direct and indirect requirements are identified and that compliance management forms part of the overall governance framework.

If there are published standards that align with or support management of compliance with specific requirements, careful consideration should be given to drawing on those standards as the foundation from which strategies can be implemented. The ISO 28001:2007 standard, "Security Management Systems for the Supply Chain—Best Practices for Implementing Supply Chain Security, Assessments, and Plans—Requirements and Guidance," is a good example of a published standard that can be readily adapted for other applications. Although the title makes reference to the "supply chain," the principles embodied in the standard are substantially universal and could be used to guide protective security compliance within other sectors that do not have the same available resources.

It may appear obvious that a well-conceived and implemented program for managing security-related risks is essential for all private and public sector enterprises. The increasing frequency of litigation and regulatory prosecutions related to security risk management (or the lack thereof) highlights the need to have a defensible basis for your security program.

Where specific security program requirements form part of broader regulatory compliance obligations, these demands must be carefully considered in the context of the other security-related risks and must be managed in a proactive manner.

Organizations should avail themselves of the resources available through regulatory agencies, standards bodies, and industry associations and ensure that the security program is able to respond to changes in the regulatory environment.

RESOURCES

A dedicated clearinghouse of information, resources, and links related to security standards, regulations, and guidelines is being established at *http://clearinghouse.amtac.net* to maintain the accuracy of links referenced in this chapter.

REFERENCES

[1] NRC. Domestic safeguards regulations, guidance, and communications; 2004 Available at http://www.nrc.gov/security/domestic/reg-guide.html.

[2] Queensland Department of Industrial Relations. Guide: Personal security in the retail industry; 2004; Available at http://www.deir.qld.gov.au/workplace/resources/pdfs/retailsec_guide2004.pdf.

[3] Legislative Assembly of Ontario. Bill 168, Occupational Health and Safety Amendment Act (Violence and Harassment in the Workplace); 2009; Available at http://www.ontla.on.ca/web/bills/bills_detail.do?locale=en&BillID=2181&BillStagePrintId=4499&btnSubmit=go.

[4] Ministry of Labour, Ontario. Workplace violence and harassment: Understanding the law; 2010; Available at http://www.labour.gov.on.ca/english/hs/pubs/wpvh/index.php.

[5] International Standards Organization. ISO31010: 2009, Risk management—Risk assessment techniques; 2009; Available at http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43170.

[6] Canadian Standards Association. CAN/CSA-Q850–97, Risk management: Guideline for decision makers; 1997; Available at http://shop.csa.ca/en/canada/risk-management/cancsa-q850-97-r2009/invt/27003271997/.

[7] SAI Global. AS/NZS 4360: 2004 Risk management; 2004; Available at http://infostore.saiglobal.com/store/Details.aspx?productID=381579.

[8] ACT. Bus services minimum service standards; 2009; Available at http://www.tams.act.gov.au/__data/assets/pdf_file/0018/143019/BusAccreditationMSS_-_Part_3_-_Mar_09.pdf.

[9] New Zealand Privacy Commissioner. Privacy and CCTV: A guide to the Privacy Act for businesses, agencies and organisations; 2009; Available at http://privacy.org.nz/privacy-and-cctv-a-guide-to-the-privacy-act-for-businesses-agencies-and-organisations.

[10] Attorney-Generals Department. Protective Security Policy Framework downloads; 2010; Available at http://www.ema.gov.au/www/agd/agd.nsf/Page/ProtectiveSecurityPolicyFramework_ProtectiveSecurityPolicyFrameworkDownloads.

CHAPTER

17

Information Technology Systems Infrastructure*

Thomas Norman, CPP

INTRODUCTION

This may be one of the most important sections in the book. The designer who does not thoroughly understand Transport Control Protocol/Internet Protocol (TCP/IP) is at a severe disadvantage in design, in construction management, and in system commissioning. The designer is at the mercy of installers and physics, both of which can harm him or her. Not understanding TCP/IP is like not being able to read or write. This is not a comprehensive tome on TCP/IP. I suggest that the reader buy several other books on the subject. This description is intended for the novice designer.

BASICS OF TCP/IP AND SIGNAL COMMUNICATIONS

TCP/IP is the basic protocol of digital systems. From the understanding of that protocol, all knowledge about digital systems flows.

How TCP/IP Works

The purpose of TCP/IP is to guide information from one place to another on a digital network.

In the beginning, when computers were owned only by the government, military, universities, and really big business (banks and insurance companies), computers were not networked. Universities and the military held discussions on how to network their machines. The first network, called ARPANET, was developed in 1969 using Network Control Protocol, an early predecessor to TCP/IP. Although this permitted limited communications, several problems were evident, mainly that computers could only talk to other computers of the same manufacturer using the same operating system and software. This was not good since the whole idea was to allow communication, not to limit it. After several iterations, TCP/IP evolved. I will not go into the entire long story; you can look that up on Google under "TCP/IP history." TCP/IP is really two separate protocols. TCP is the Transport Control Protocol, and IP is the Internet Protocol. TCP was developed in 1974 by Kahn and Cerf and was introduced in 1977 for cross-network connections. TCP was faster, easier to use, and less expensive to implement. It also ensured that lost packets would be recovered, providing quality of service to network communications. In 1978, IP was added to handle routing of messages in a more reliable fashion. TCP communications were encapsulated within IP packets to

*Originally from Norman, T. Integrated security systems design. Boston: Butterworth-Heinemann, 2007. Updated by the editor, Elsevier, 2011.

ensure that they were routed correctly. On the receiving end, the TCP packets were unpacked from their IP capsules. Experts quickly realized that TCP/IP could be used for virtually any communication medium, including wire, radio, fiber, and laser, as well as other means. By 1983, ARPANET was totally converted to TCP/IP, and it became known as the Internet.

TCP/IP Operates on Open Systems Interconnection Levels 3 (IP) and 4 (TCP)

One of the basic functions of networking involves the process of layering communications. Like making a sandwich, one cannot begin by spreading mayonnaise on one's hand. You have to put it on bread. Then you add the meat, lettuce, pickles, and so forth, and finally a last layer of bread. Network communications are like that. To send a packet of video, audio, or data, one must build up a series of layers. At the other end, those layers are taken off until the packet is ready for viewing or listening. There are seven layers to the Open Systems Interconnection (OSI) reference model. Each layer adds a protocol. Dick Lewis (Lewis Technology, *www.lewistech.com/rlewis/Resources/JamesBondOSI2.aspx*) uses an example of James Bond to describe how the seven layers work (Figure 17-1). The following is his description:

> *James Bond meets Number One on the seventh floor of the spy headquarters building. Number One gives Bond a secret message that must get through to the U.S. embassy across town.*
>
> *Bond proceeds to the sixth floor, where the message is translated into an intermediary language, encrypted, and miniaturized.*
>
> *Bond takes the elevator to the fifth floor, where security checks the message to be sure it is all there and puts some checkpoints in the message so his counterpart at the U.S. end can be sure he's got the whole message.*
>
> *On the fourth floor, the message is analyzed to see if it can be combined with some other small messages that need to go to the U.S. end. Also, if the message was very large it might be broken into several small packages so other spies can take it and have it reassembled on the other end.*

7 Layers of the OSI Model

Layer #	Layer	Functions	Methods	Transmit	Receive
7	Application	Communication Partners Identified, Quality of Service Identified, User Authentication, Data Syntax	E-Mail, Network Software, Telnet, FTP	⇩	⇧
6	Presentation	Encryption	Encryption Software	⇩	⇧
5	Session	Establishes and Terminates Network Sessions between Devices and Software Requests	CPU Process	⇩	⇧
4	Transport	Error Recovery and Flow Control	CPU Process	⇩	⇧
3	Network	Switching and Routing, Network Addressing, Error Handling, Congestion Control, and Packet Sequencing	Switcher, Router	⇩	⇧
2	Data Link	Data Packets Encoded/Decoded into Bits	Media Access Control (MAC) and Logical Link Control (LLC)	⇩	⇧
1	Physical	Electrical, Light, or Radio Bit Stream	Cables, Cards, Ethernet, RS-232, ATM, 802.11a/b/g	⇩	⇧

FIGURE 17-1 OSI layers.

The third-floor personnel check the address on the message and determine who the addressee is and advise Bond of the fastest route to the embassy.

On the second floor, the message is put into a special courier pouch (packet). It contains the message, the sender, and destination ID. It also warns the recipient if other pieces are still coming.

Bond proceeds to the first floor, where Q has prepared the Aston Martin for the trip to the embassy.

Bond departs for the U.S. embassy with the secret packet in hand. On the other end, the process is reversed. Bond proceeds from floor to floor, where the message is decoded.

The U.S. ambassador is very grateful the message got through safely.

"Bond, please tell Number One I'll be glad to meet him for dinner tonight."

The important point to understand is that in any network today, each packet is encapsulated (enclosed) seven times and, when received, is decapsulated seven times. Each encapsulation involves checking and packaging to make the trip a sure and safe one for the data. Each decapsulation reverses that process:

- Data begins its trip at layer 7, the application layer, which includes software programs, Microsoft Word™, and so forth.
- It is passed down to layer 6, the presentation layer, which adds data compression, encryption, and other similar manipulations of the data.
- It is then passed down to layer 5, the session layer, which provides a mechanism for managing the dialog between the two computers, including starting and stopping the communications and what to do if there is a crash.
- From there, it goes to layer 4, the transport layer (TCP), which ensures reliable communications between the machines. The packet changes from data to segments in the TCP layer.
- Down to layer 3, the network layer (IP), where error control and routing functions are described. The segments are combined or broken up into defined-sized packets at the IP layer. Routers are layer 3 devices.
- Down to layer 2, the data link layer, where functional and procedural means to transfer data between network entities and detection and correction of errors that could occur on the lowest layer take place. It is on this layer that the addressing of exact physical machines, each with its own media access control (MAC) address, is found. Each digital device attached to any network has its own unique MAC address, allowing sure identification that the device is authorized for connection to the communication or network. Network switches are layer 2 devices.
- Finally, down to layer 1, the physical layer, which includes cable, voltages, hubs, repeaters, and connectors.

TCP/UDP/RTP

One of the major advantages of TCP/IP is that it is able to fix bad communications. It does this by keeping track of packet lists for a given communication. Andrew G. Blank, author of *TCP/IP Foundations*,[1] uses a wonderful illustration of a children's soccer team at a pizza parlor with an attached game arcade:

Let's say that I take my son's soccer team to an arcade and restaurant for a team party. I have the whole team outside the arcade. My task is to get the team to the other side of the arcade, to my wife who is waiting for them in the restaurant. In this analogy, the team represents the complete

[1]This book is no longer available, but references to it still exist on a number of Internet Web pages, most notably on www.wikipedia.com under the search string "OSI model."

file on one host, and each child represents a data packet. One of my goals is to lose as few of the kids as possible.

While we are standing outside, it is easy to put the team in order; all the children are wearing numbered jerseys. I tell the kids that we will meet on the other side of the arcade in a restaurant for pizza and that they should all move as fast as possible through the arcade and to the restaurant.

After I open the door and say "Go," the kids enter one at a time. Entering the arcade one at a time represents the fragmenting and sending of the file. Just as each of the kids has a numbered jersey, each packet has a number so that the receiving host can put the data back together.

Now picture a dozen 6-year-olds moving through the arcade. Some of the children will take a short route; others will take a long route. Possibly, they'll all take the same route, though it is much more likely that they will all take different routes. Some will get hung up at certain spots, but others will move through faster. My wife is in the restaurant waiting to receive the team. As they start arriving at the restaurant, she can reassemble the children (packets) in the correct order because they all have a number on their backs. If any are missing, she will wait just a bit for the stragglers and then send back a message that she is missing part of the team (file).

After I receive a message that she is missing a child (a packet), I can resend the missing part. I do not need to resend the entire team (all the packets), just the missing child (packet or packets).

Please note, however, that I would not go look for the lost child; I would just put the same numbered jersey on a clone of the lost child and send him into the arcade to find the restaurant.

TCP is designed to reconstruct lost packets so that an entire communication is intact. This is very important for files such as employee records, word processing files, and spreadsheets, where a missing packet can cause the whole file to be unreadable.

USER DATAGRAM PROTOCOL

For video and audio, another protocol is required. TCP can cause problems with audio and video files because its attempt to resend lost packets results in portions of the communication occurring out of place and therefore in the wrong sequence, making the video or audio communication intelligible. The human eye and ear are very good about rebuilding lost portions of communications. Imagine a restaurant in which you are overhearing a conversation at an adjacent table. You may not be able to hear the entire conversation—not every word because of the noise from others talking—but you can still follow what is being said.

Instead, what we need is a protocol that will send the data without error correction and without attempting to resend lost packets. That protocol is the User Datagram Protocol (UDP). UDP is called a connectionless protocol because it does not attempt to fix bad packets. It simply sends them out and hopes they arrive. The transmitting device has no way of knowing whether they do or not.

UDP and its partner, Real-Time Protocol (RTP), work together to ensure that a constant stream of data (hence the term "streaming data") is supplied for a receiving program to view or hear. RTP is used for audio and video. Typically, RTP runs on top of the UDP protocol.

As an industry default, all network data is called TCP/IP data, whether it is TCP/UDP or RTP. It is kind of like calling any tissue Kleenex™ or any copier a Xerox™ machine. It is not accurate; it is just that everyone does it.

Another important set of protocols that security designers will need to know about are unicast and multicast protocols. These are discussed in detail later in this chapter.

TCP/IP Address Schemes

Each network device has a network card that connects that device to the network. The network interface card (NIC) has a MAC address and a TCP/IP address to identify itself to the network. The MAC address is hardware assigned at the factory when the device is manufactured. It can never be changed. The TCP/IP address is assignable, and it defines where in the network hierarchy the device is located. TCP/IP addresses are used to ensure that communications errors do not occur and that the address represents the logical location on the network where the device resides. TCP/IP addresses are like postal addresses, which identify where a house is on what street, in what neighborhood, in what city, in what state, and in what country. MAC addresses are like the name of the person who resides in the house. The MAC address will change if one replaces a computer with another, but the TCP/IP address can stay the same on the network for the user of the computer so that all messages to that user, worldwide, do not need a new MAC address in order to reach him or her.

There are two versions of TCP/IP addresses, which are known as IPv4 and IPv6. IP version 4 was the original version under which the whole Internet worked until it was determined that the number of available addresses would soon run out. So a larger array of numbers was defined, called IP version 6. IPv6 can accommodate a very large (virtually infinite) number of connected devices.

In IPv4, addresses are broken down into what is called decimal notation for the convenience of the user. Remember, each address is actually a series of binary data (ones and zeros), but they are grouped together in a fashion that is much easier to understand. Four groups are combined together, separated by decimals. Each group (byte) can be a number from 0 to 255 (a total of 256 numbers). This is an 8-bit value. A typical address can be from 0.0.0.0 to 255.255.255.255. IPv4 provides for in excess of 4 billion unique addresses. IPv6 replaces the 8-bit value with a 12-bit value. (0.0.0.0 to 4095.4095.4095.4095). The IPv6 address range can be represented by a 3 with 39 zeros after it. It is a large number. IPv4 is still adequate for today's networks, but IPv6 is coming.

Briefly, the first one or two bytes of data, depending on the class of the network, generally will indicate the number of the network. The third byte indicates the number of the subnet and the fourth byte indicates the host (device) number on the network. The host cannot be either 0 or 255. An address of all zeros is not used, because when a machine is booted that does not have a hardware address assigned to it, it provides 0.0.0.0 as it addresses until it receives its assignment. This would occur for machines that are remote booted (started up) or for those that boot dynamically using the Dynamic Host Configuration Protocol (DHCP). The part of the IP address that defines the network is called the network ID, and the latter part of the IP address is called the host ID.

Regarding the use of automatic or manual device addressing, we recommend manual addressing for security systems. DHCP incurs the possibility of security breaches that are not present with static addressing.

NETWORKING DEVICES

Security system digital networks are composed of five main types of network devices.

Edge Devices

Edge devices include digital video cameras, digital intercoms, and codecs. These are the devices that, for the most part, initiate the signals that the rest of the system processes. One exception to this is that codecs can also be used to decode digital signals and turn them back into analog signals for viewing of digital video signals or listening to digital audio signals. The most common use of the decoding codec is for security intercoms, where an analog intercom module is a must in order to hear and speak from the console.

Communications Media

Digital signals are communicated along cable or wirelessly. The most common type of wired infrastructure is an Ethernet cabling scheme. Although other types exist (ring topology, etc.), none are prevalent. Ethernet is a wired scheme

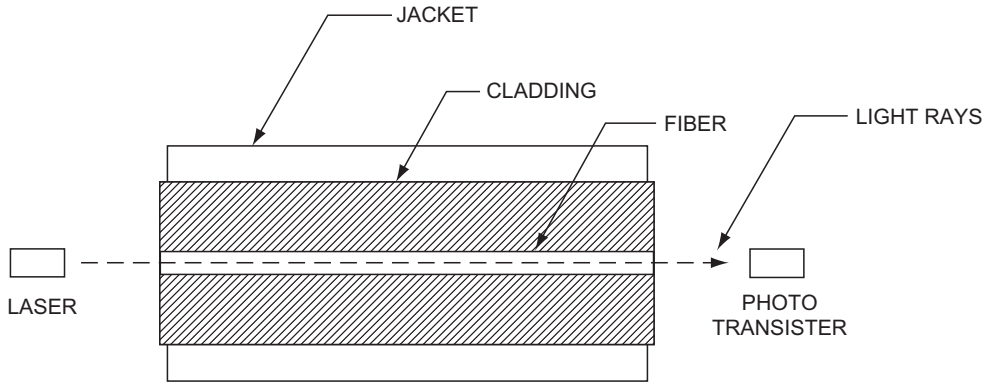


FIGURE 17-2 Single-mode fiber.

that allows many devices to compete for attention on the network. It is designed to handle collisions that occur when two or more devices want to talk simultaneously.

Devices contend for attention and are granted permission to speak while all other devices listen. Contention can slow a network, reducing its throughput. A network can be segmented by switches and routers to reduce contention and regain efficiency.

Ethernet is defined under IEEE[2] Standard 802.3. Ethernet classes vary by speed, with the slowest being 10Base-T [10 megabits per second (Mbps)]. Fast Ethernet is called 100Base-T and operates at 100 Mbps. Gigabit or 1000Base-T operates at 1 gigabit per second (Gbps). Wiring distances depend on wire type and speed. Ethernet is wired using unshielded twisted pair (UTP) four-pair wiring on RJ-45 connectors. Category 5 or 5e (Category 5 Enhanced) wiring is used for 10Base-T, 100Base-T, and 1000Base-T (up to 328 ft). Category 6 wire is useful for 1000Base-T runs up to 328 ft. For 1000Base-T connections, all four pairs are used, whereas for 100Base-T connections, only two pairs of wires are used.[3]

Category 5, 5E, and 6 cables use four pairs, where the colors are

- Pair 1—white/blue
- Pair 2—white/orange
- Pair 3—white/green
- Pair 4—white/brown

The second most common type of wired infrastructure is fiber optic. These come in two types: single mode and multimode. When told that the difference between the two is the number of signals they can carry, newbies often think that the single mode will carry one and the multimode will carry more. In fact, just the opposite is true.

Single-mode fiber is based on a laser, whereas multimode may use either a laser or a light-emitting diode (LED) for a signal source (Figure 17-2). Multimode fiber is typically plastic, whereas single-mode fiber is made of glass. Multimode fiber has a large cross-sectional area relative to the wavelength of the light transmitted through it, typically either 50 or 62.5 μm (micron) fiber diameter compared to 1.3 μm for 1300 nm modulated light frequency. Accordingly, multimode bounces the light off the inside of the fiber (Figure 17-3). As the light bounces off the walls of the fiber, it takes many different paths to the other end, which can result in multiple signals at the other end. The result is a softening or rounding of the square digital signal. Over distance, the signal becomes more difficult to read at the receiver—thus the limited distance of multimode fiber.

[2]The Institute of Electrical and Electronics Engineers (IEEE) is the world's leading professional association for the advancement of technology.

[3]Hewlett-Packard, 1000Base-T gigabit Ethernet tutorial, September 15, 2000. Available at http://www.docs.hp.com/en/784/copper_final.pdf.

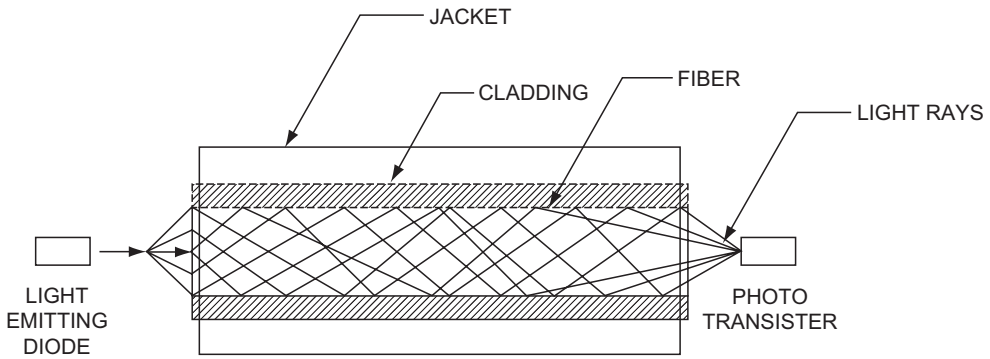


FIGURE 17-3 Multimode fiber.

Distance is also a factor of bandwidth. You can use multimode at longer distances with less speed. Fast Ethernet (100 Mbps) can travel farther than gigabit Ethernet (1000 Mbps). Check the manufacturer's specification sheets both for the fiber and for the transceivers you intend to use for exact limits based on speed.

Single-mode fiber is made of glass, and it pipes the laser directly down the middle of the glass tube like a waveguide.[4] This is because single-mode fiber has a small cross-sectional area (8 or 9 μm) relative to the frequency of the light transmitted through it (1.3 μm at 1300 nm). The laser can carry multiple signals on its carrier.

The most commonly used frequencies are 1550, 1310, and 850 nm. The 1550 and 1310 nm frequencies are very common to single-mode fiber, and 850 nm is most commonly used in multimode fiber. The 1310 and 1550 nm frequencies are exclusively transmitted using lasers, and the 850 nm frequency is exclusively transmitted using LEDs. By using multiple frequencies (1310 and 1550 nm), it is possible to transmit and receive bidirectionally over a single fiber. Although this is not a common practice, some transceivers can accommodate two frequencies on a single fiber, especially with single-mode fiber. Typically, 1300 nm is used to send and 1550 nm is used to receive at one end and vice versa at the other end. More commonly, bidirectional communication is accommodated by using two separate fibers on the same frequency. No standard has been developed for multiple frequencies on a single fiber on multimode cable, but at least one security fiber optic company has developed a fiber optic media converter that can both transmit and receive on a single multimode fiber using two separate frequencies.[5]

Manufacturers have long since surpassed the IEEE 802.3z standard in terms of the distances served. Multimode fiber distances are typically limited to 1640 ft for fast Ethernet connections. Gigabit speeds are commonly limited to 1000 ft.

[4]A waveguide is a structure that guides very high-frequency radio waves (radar, microwave, etc.) down a tube from a transmitter to an antenna or from a receiving antenna to a receiver. Above normal radio frequencies, conventional wires are useless for carrying the signal because of the "skin effect." The skin effect is an effect of physics that results in radio waves traveling increasingly closer to the outside of a conductor as the frequency rises, eventually losing connection with the conductor altogether. Above that frequency, a waveguide must be used to contain the transmission because normal wiring is unusable. The low-frequency cutoff of a waveguide is half of the wavelength of the frequency being passed. Generally, waveguides are useful above 1 GHz.

[5]The American Fibertek 47-LX series 1000Base-LX Ethernet Fiber Optic Media Converter uses a single multimode fiber and transmits and receives on two frequencies (1310 and 1550 nm). This company also makes a 100Base-LX converter "45-LX series." Both units use a laser to transmit and receive on a single multimode fiber. This company also makes LED two-fiber single-mode and multimode solutions, as do many other firms.

Single-mode fiber distance limitations vary and can commonly be 43–62 miles with economical equipment;[6] much farther distances are possible (up to 500 miles) with more sophisticated media converters.[7] With commonly available equipment, it is possible to achieve distances of up to 93 miles with single-mode or multimode at 100Base-T speeds and 75 miles at 1000Base-T speeds.[8]

Lastly, single-mode transceivers and fiber are more costly than their comparable multimode equivalents. The cost delta can be vast. Use multimode for shorter distances (e.g., on a campus) or where cost is a factor. However, the cost delta can sometimes be worth it if there is available single-mode fiber in the ground on a campus and the only cost to mount up the system is that of the transceivers.

Gigabit switches and routers are usually supplied with single- or multimode fiber ports. This is the preferred connectivity method over the use of separate transceivers.

TCP/IP signals can also be communicated via radio, microwave, or laser. The most common type of radio communication network is in the 802.11 band. 802.11 is available in two major categories: backhaul or client service. The backhaul type is delivered by 802.11a, whereas client services are often provided by 802.11b/g/i. 802.11a makes available 10 channels, and with the correct antennas one can use all 10 channels in the same airspace. 802.11b/g/i are very similar but differ by the bandwidth provided and the level of security implemented. 802.11b provides 11 Mbps maximum, whereas 802.11g/i provide 54 Mbps. It is possible to find 802.11g devices that provide 108 Mbps. These are full-duplex devices that use a separate transmitter and receiver to double the bandwidth. This function is very common in 802.11a, which also provides 54 Mbps per available channel. 802.11b/g/i have 13 available channels, but cross-traffic is a problem. Do not plan to use more than 6 channels in a single airspace.

[6]Cisco Gigabit Interface Converter 1000Base-ZX GBIC media converter using premium single-mode fiber or dispersion shifted single-mode fiber.

[7]Goleniewski, L. Telecommunication essentials: The complete global source for communications fundamentals, data networking and the Internet, and next generation networks. Reading, MA: Addison-Wesley, 2001.

[8]For example, FibroLAN TX/FX H.COM 10/100 provides 100Base-T speeds up to 93 miles (150 km) over single mode or multimode. Their GSM1000 and GSM1010 provide gigabit speeds up to 75 miles (120 km) over single mode or multimode. Prices vary from a few hundred to a few thousand dollars, depending on the range required.

NETWORK INFRASTRUCTURE DEVICES

Network infrastructure devices comprise those devices that facilitate the movement of data along the communications media. Digital cameras and codecs connect to a digital switch in order to get on the network.

Hubs

The most basic type of network device is a hub. A hub is simply a device with Ethernet connectors that connects all devices together in parallel with no processing. A few hubs have power supplies and provide LEDs to indicate port activity, but do not confuse this with active electronics. Hubs are dumb. Hubs have no ability to control the collisions that naturally occur in Ethernet environments, so when too many devices are connected together on a hub, the network throughput suffers due to delays caused by the collisions. It is inadvisable to use a hub for all but the simplest networks (less than eight devices). Hubs offer no security services, are OSI level 1 devices, and connect devices.

Switches

A switch is a smart hub. Unlike a hub that presents each signal to all connected devices, a switch is able to read the TCP/IP packet header and direct the signal to the appropriate port(s). Switches are OSI level 2 devices and control where data may go.

Routers

Routers are one step up from switches. In addition to directing the traffic of individual ports, they can in fact make decisions about data that is presented to them and can decide if that data belongs on that section of the network. Routers can create subnets of the greater network. This allows functions and devices to be segmented into logical groups. Subnets reduce the overall amount of network traffic, making the network operate more efficiently. Subnets can be used to separate different sites, campuses, and buildings and are sometimes even used to separate edge devices from client workstations. Routers control what data may go.

Firewalls

Firewalls are used with routers to deny inappropriate data traffic from another network. Firewalls can be configured in either hardware or software. Security systems that are connected to any other network should be connected through a firewall. Otherwise, a security system is not secure and, thus, the facility will not be secure. Firewalls deny malicious data.

Intrusion Detection Systems

Intrusion detection systems (IDSs) can also be either hardware or software devices. They continuously monitor the traffic into and out of the network to detect any unauthorized attempt to gain access to the network. The IDS will warn the network administrator of the attempt and provide insight into how the attack attempt was executed in order to adjust the firewall to limit future attempts using that method. IDSs warn the system administrator about attempts to probe the network or insert malicious data.

SERVERS

Servers process and store data for use by workstations. For security systems, there are several possible types of servers. These may be combined on a single machine or may be distributed across several physical servers.

Directory Service Server

The directory service is an index for all workstations to use to find the data for which they are searching. It tells them where to find the correct camera, intercom, or archive stream. Additional functions may include Internet information services (IISs), domain name service (DNS), and other network management services.

Archive Service

The archive server stores data for future reference.

Program Service

The program service allows programs to reside on the server rather than on the workstation. This is not recommended because the few dollars saved results in a slower system.

FTP or HTTP Service

This is very useful for remote monitoring and retrieval of data from a remote site to a central monitoring station, for example, or for a manager to “look in” on a site.

E-Mail Service

Servers can send or manage e-mail.

Broadcast Service

Servers can broadcast alerts or alarms to pagers, cell phones, loudspeakers, printers, and so forth.

Workstations

Workstations provide a human interface to the network. Workstations can be single purpose or multiuse, serving other types of programs and other networks. For large sites, it is often best to use single-purpose machines on a dedicated

network. Workstations can support many video monitors in order to display digital video, alarm/access control, intercom, report and analysis software, browser, and so forth. We often design systems that have up to six monitors per workstation. It is also possible to operate more than one workstation with a single keyboard and mouse in order to support more functions than a single workstation can handle. This is often necessary for systems that do not prioritize intercom audio over video.

Printers

Printers can be connected to a workstation or directly to the network, where they can serve multiple workstations.

Mass Storage

Digital video systems can store a lot of data—much more data than any other type of system. It is not unusual for us to design systems with many terabytes of video storage. This amount of storage cannot be contained in a single server or workstation. There are two ways of extending the storage: network attached storage (NAS) and storage area networks (SANs). The names are so similar that they can be confusing, but the differences are extensive.

NAS units include a processor and many disk or tape drives (or a combination of both). They are typically configured to "look" like a disk drive to the system, and they connect directly to the network, just like a server or a workstation. This means that a large volume of data traffic is on the network to feed the NAS.

A SAN is on its own network in order to separate the vast amount of traffic it generates away from the common network. This is a good idea, even for small systems. SANs can be created easily by adding a second NIC to the archive server and connecting the SAN to that NIC.

NETWORK ARCHITECTURE

Simple Networks

The simplest networks connect two devices together on a cable (Figure 17-4). Basic networks connect several devices together on a single switch. This creates a local area network (LAN) (Figure 17-5). From there, tree architecture is common. There may be a single workstation/server (one computer serving both purposes) that is connected through one or more switches to a number of cameras, intercoms, codecs, access control panels, and so forth (Figure 17-6).

Advanced Network Architecture

Backhaul Networks. Beyond simple tree architecture, as network size grows, it is common to create a backhaul network and a client network. This can be achieved in its simplest form with gigabit switches. A simple gigabit switch is equipped with a number of fast Ethernet (100 Mbps) ports to connect edge devices, such as cameras, codecs,

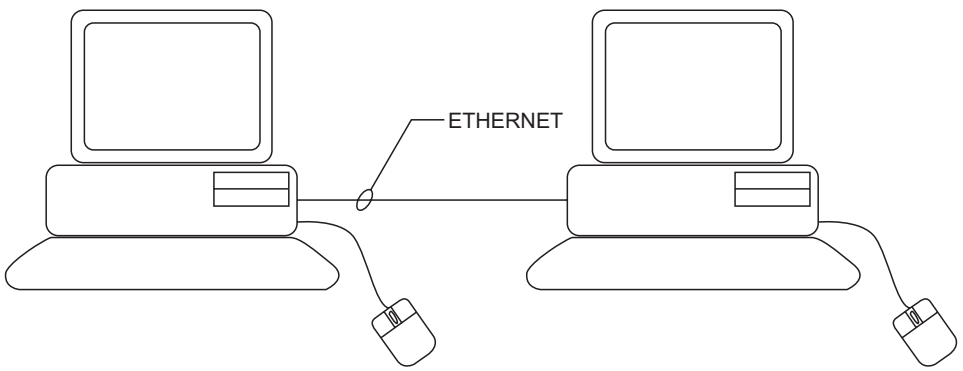


FIGURE 17-4 Simple network.

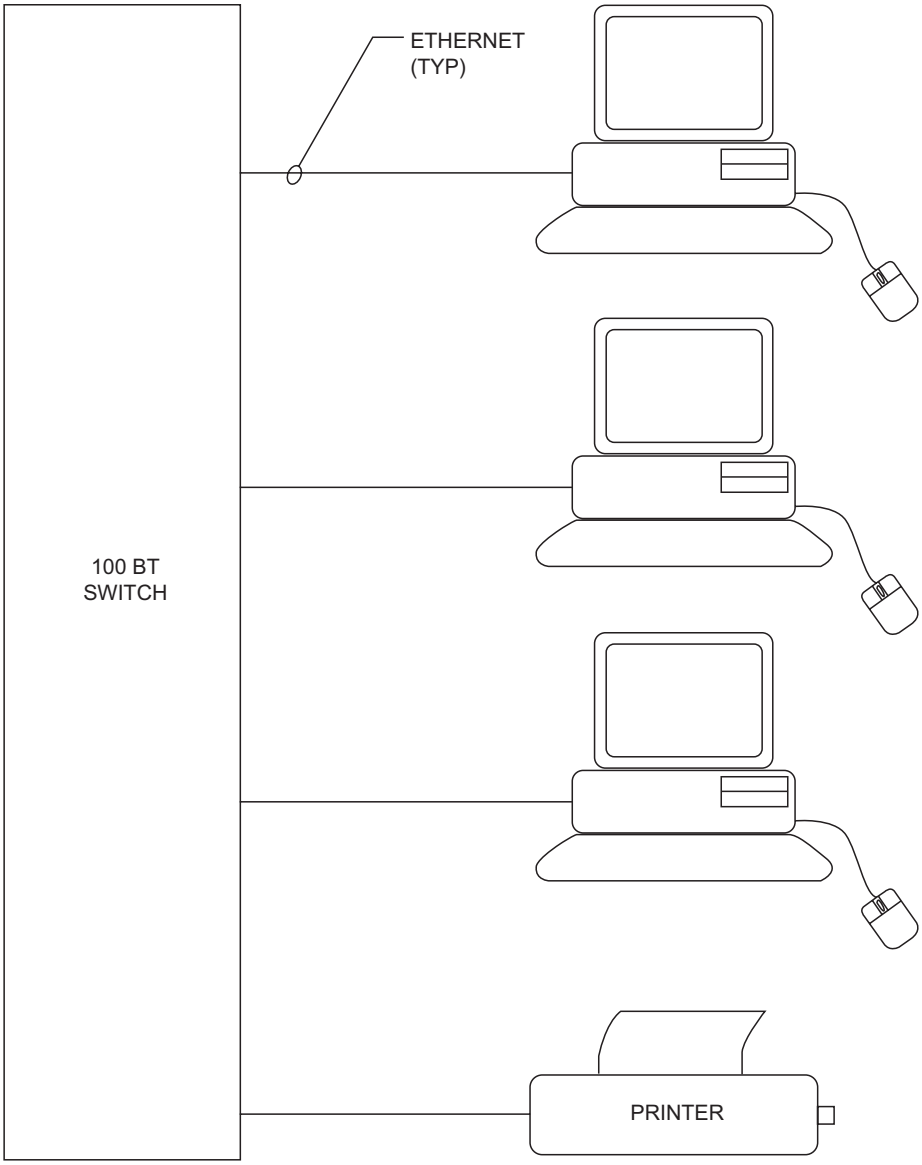


FIGURE 17-5 Switch connected network.

intercoms, or access control panels, and a backhaul connection that supports gigabit (100 Mbps) speeds.

The result looks like an organization chart in which the server/workstation is at the top on the gigabit backhaul network and the edge devices (clients) are on the 100 Mbps ports of the switches (Figure 17-7).

Subnets. A subnet is basically virtual LAN (VLAN) that is a logical subset of the overall LAN.

Subnets are used for several reasons, the most common of which are to limit network bandwidth to manageable levels or to minimize traffic that is not appropriate for certain devices, such as segregating buildings on a campus.

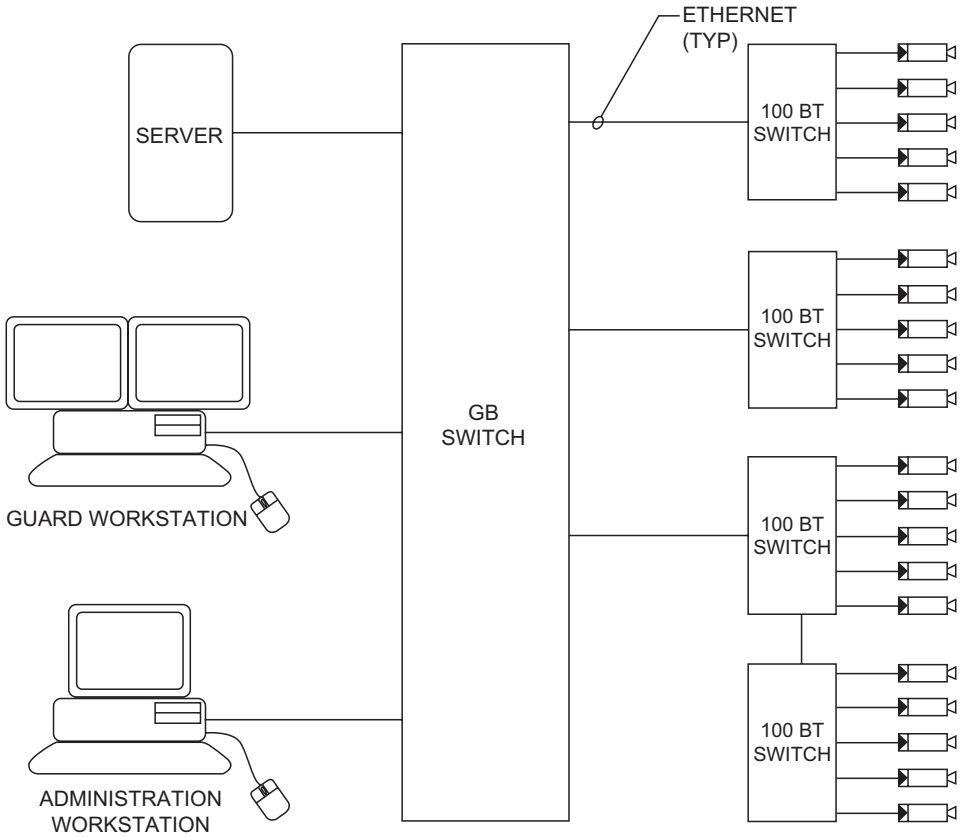


FIGURE 17-6 Simple tree network.

Subnets to Limit Network Traffic. As network bandwidth increases, it can task the switches to a point at which they begin to drop packets. I recommend that you do not pipe more than 45% of the rated bandwidth of any device because the rated bandwidths are based on normal network traffic, not streaming data such as video. Stay under 45% and you will not usually experience problems. A VLAN is created by joining two or more networks by routers.

Typically, routers are placed on the backhaul network, and they in turn may have their own backhaul networks that serve many edge devices. Architected thus, no single subnet will have too much traffic on it (Figure 17-8).

Subnets to Segregate Network Traffic. When a security system serves many buildings on a campus, it is not useful to have the traffic of one building on the network of others. So each building can be joined to the main backhaul network through a router such that its traffic is limited only to data that are relevant to that building alone (Figure 17-9).

The security system could be placed on the larger organization's network as a subnet. Subnets can be integrated onto a larger network in a way that would seem by their physical connections to be blending the two networks, whereas in fact they operate as completely segregated networks, totally isolated from each other by routers and firewalls. Be advised that enterprise security systems using large amounts of digital video can tax the bandwidth of virtually any organization's business network architecture to the breaking point.

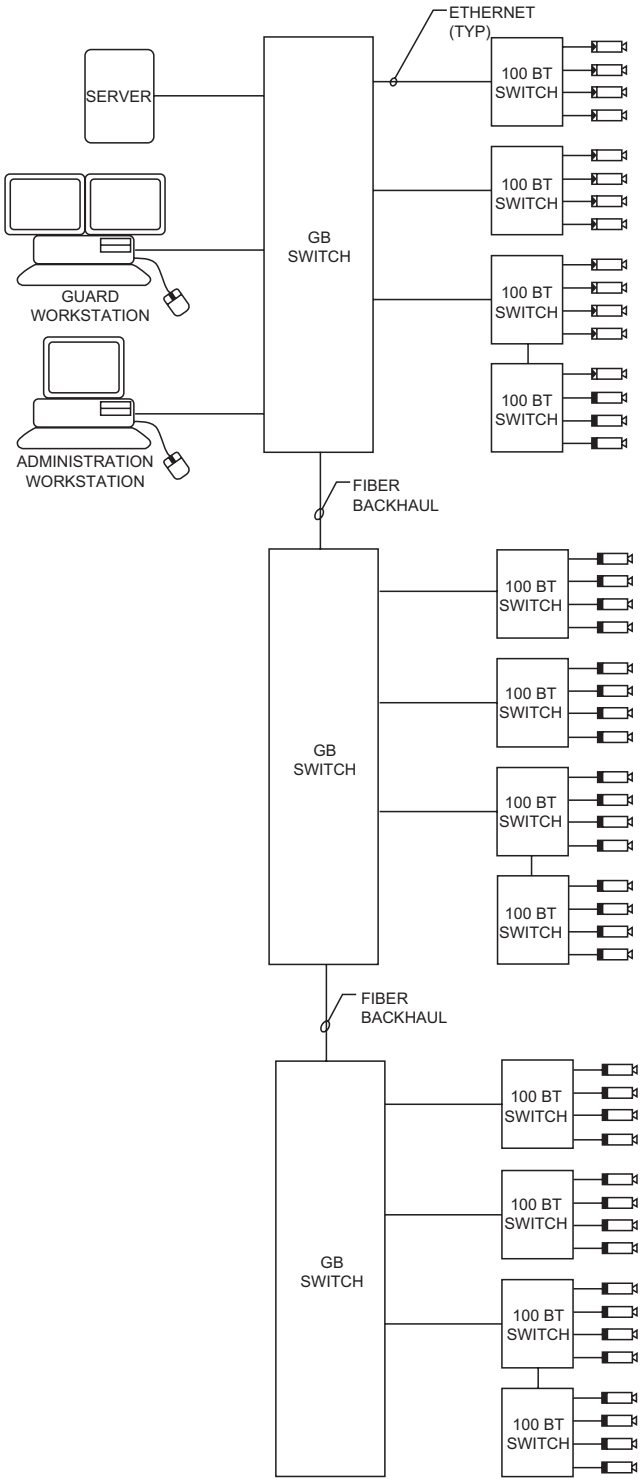


FIGURE 17-7 Backhaul network.

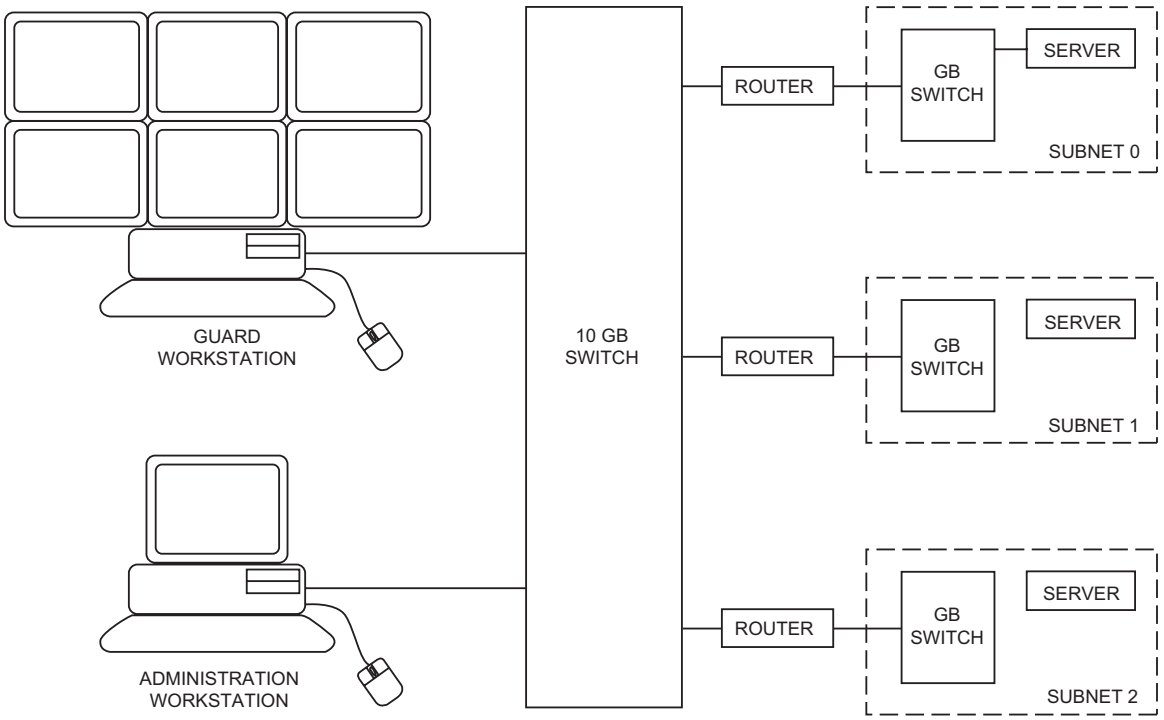


FIGURE 17-8 Subnet for limiting network traffic.

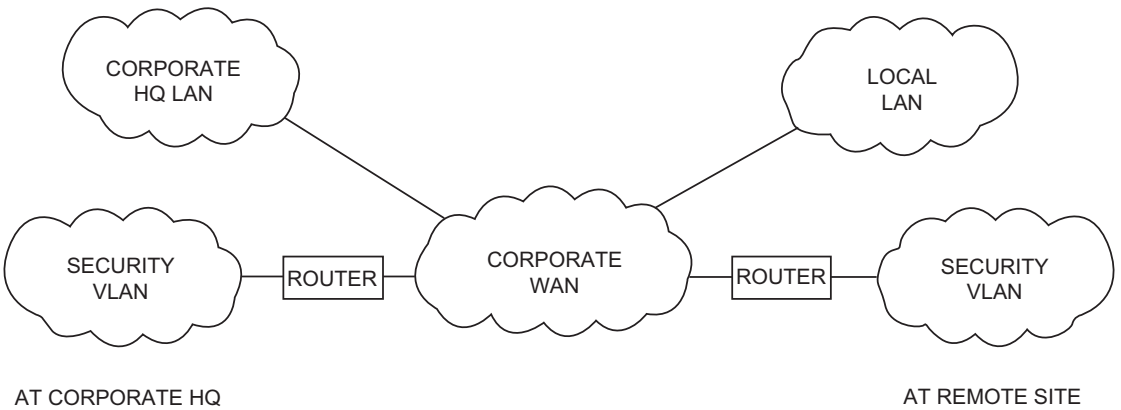


FIGURE 17-9 Subnet to segregate network traffic.

It is often advisable to physically segregate the networks. Additionally, when the security system is placed on the organization's network, significant additional effort is required to secure the security system network from the organization's network, which will never likely be as secure as the security system network, notwithstanding the assertions of the organization's information technology department (Figure 17-10).

VLANs. VLANs are global subnets. Like a subnet, a VLAN segregates a data channel for a specific purpose or group. Unlike a subnet, which is a hierarchical daughter of a physical LAN, a VLAN can coexist across the mother LAN as a

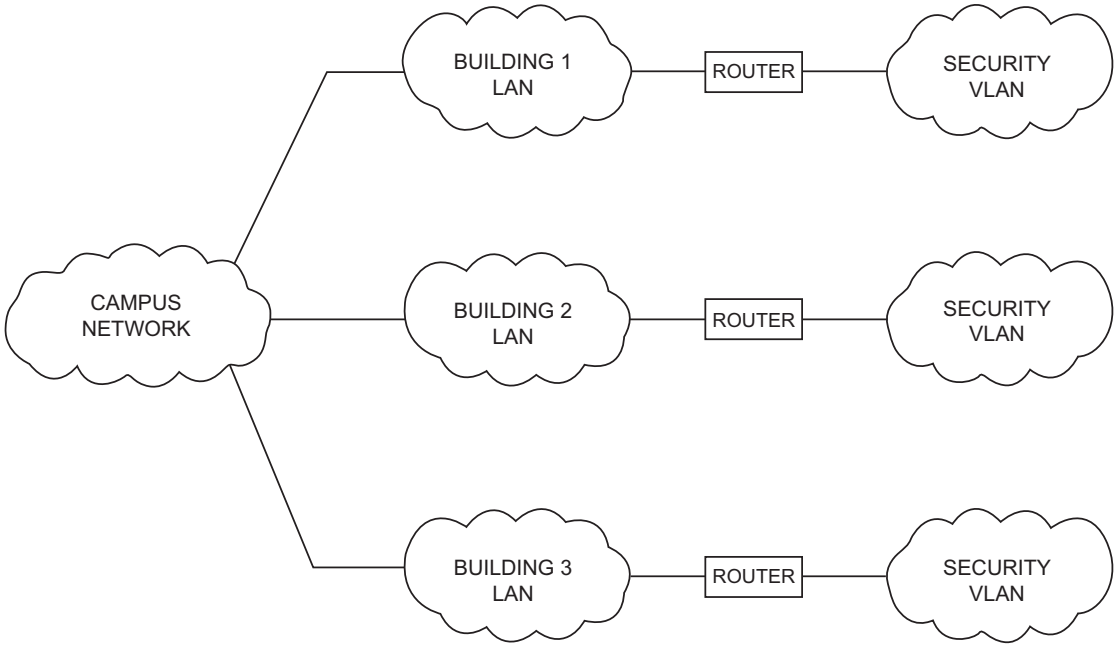


FIGURE 17-10 Subnet used to blend networks.

VLAN as though there were two separate sets of hardware infrastructure. It does this by operating on a dedicated port to which only the VLAN has privileges. Therefore, cameras, intercoms, and access control system controllers can be plugged into the same managed switch with workstations and printers of the organization's business LAN, and when the security devices' ports are dedicated to a security VLAN, those devices will not be apparent or accessible to the users or the LAN. This is one of the best methods for sharing networks between security and business units.

NETWORK CONFIGURATIONS

A network is composed of a series of TCP/IP devices connected together. There are a variety of ways to do this, and each has its own advantages and limitations.

Peer-to-Peer

The most basic network is a stand-alone peer-to-peer network. Peer-to-peer networks are created by connecting each device together through a hub or switch. Each computer, codec, or access control panel is equal in the eyes of the switch. This is adequate for very small networks (Figure 17-11).

Client/Server Configuration

As network sizes expand, a client/server configuration is preferred. Major processing is performed in one or more servers, and the human interface is accommodated with client devices or workstations (Figure 17-12). Cameras, intercoms, access control readers, locks, door position switches, request-to-exit devices, alarm-triggering devices, and so forth are all human interface devices, as are guard and lobby workstations, intercom master stations, and so forth.

Typically, the human interface devices are connected to processing devices that interface to the network via TCP/IP connection, usually Ethernet. These may include codecs and alarm/access control panels.

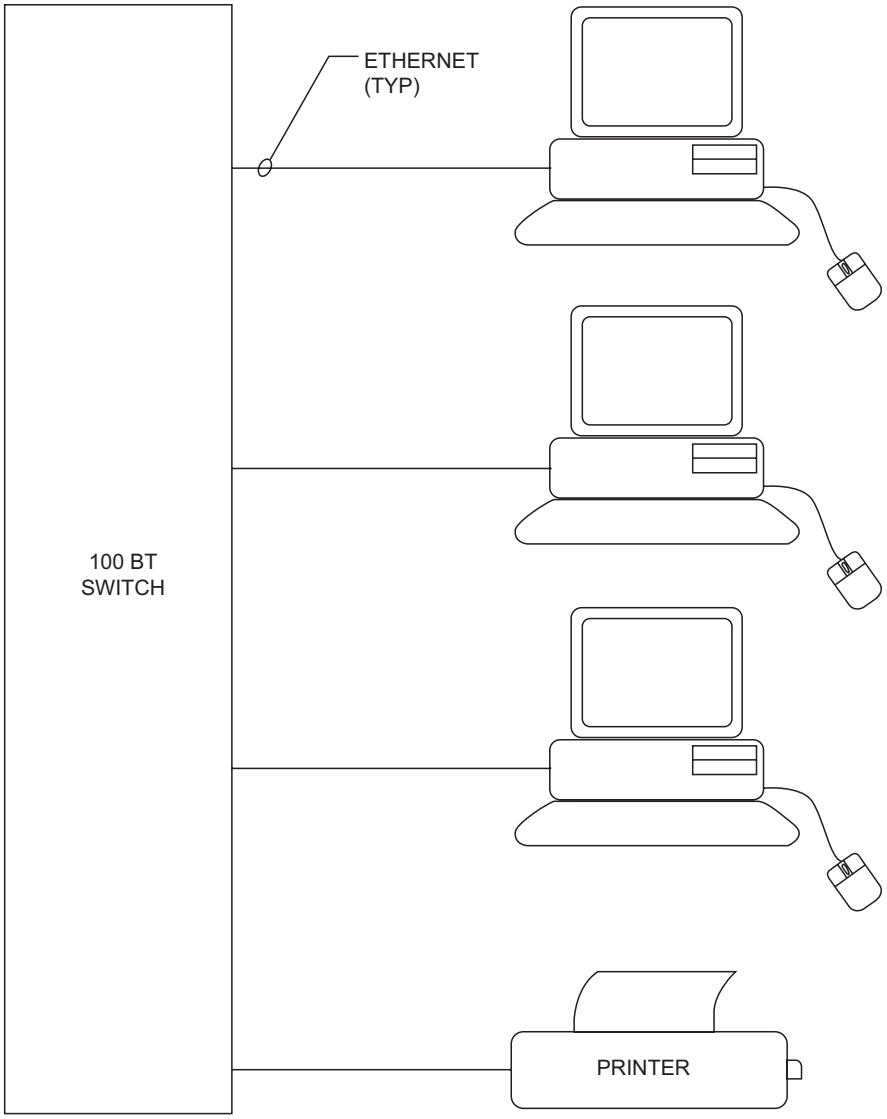


FIGURE 17-11 Peer-to-peer network.

On larger networks, it is common to use multiple servers. Commonly, there will be multiple archive servers.

It is also common to use a second set of servers as a backup to the primary servers in case of a disaster that disables the primary servers. This allows for remote access to the data up to the second of the disaster in order to analyze the event and to provide a business continuity record of all network data.

CREATING NETWORK EFFICIENCIES

One of the major advantages of enterprise security systems is the opportunity for remote monitoring of distant buildings. This often requires blending the security system network with the organization's business network.

The most common requirement is to monitor remote sites. It is not necessary to send all

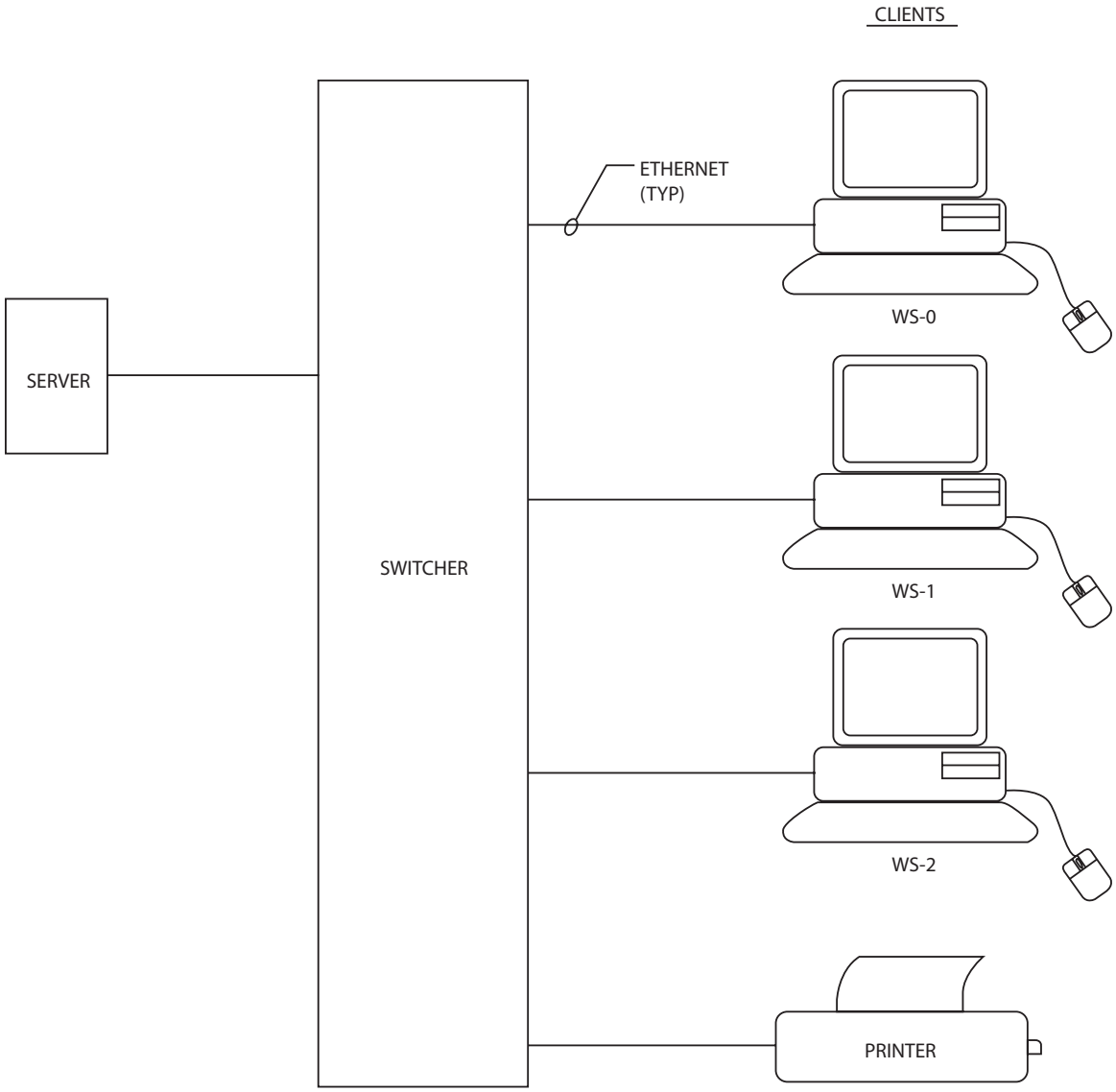


FIGURE 17-12 Client/server network.

of the data from the monitored site to the site doing the monitoring. The monitoring center only needs to see the data it wants to look at. When you are watching a sports broadcast on TV on channel 11, you do not usually care much about the opera playing on channel 4. Likewise, it is advisable to attach the remote monitoring center only to those data that are relevant at the moment. You do not need to send the video of all the cameras all the time. Using this method, great efficiencies can be gained. Overall network bandwidth can be limited only to the cameras being monitored. I use cameras as an example here because they consume the most bandwidth.

There are two very efficient ways to remotely monitor over a business network: browser and virtual private network (VPN). A browser

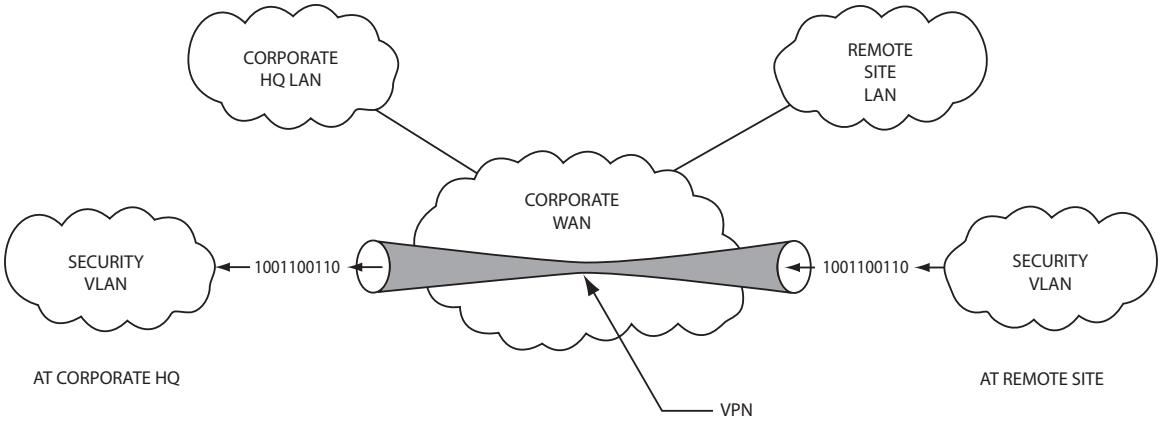


FIGURE 17-13 Virtual private network.

connection is quick, easy, and does not consume any bandwidth when it is not sending data. It consumes only what it displays. One can configure simple monitoring centers with browser connections to the remotely monitored sites. When one wants to see the site, one makes the connection; otherwise, the connection is closed. However, browser connections consume data even when minimized, whether or not the data is sent to the screen. This will consume both network bandwidth and workstation processing power. So it is advisable to close browsers when not being viewed. Alarms can be sent on a separate data link to alarm monitoring software that is always open. These consume virtually no bandwidth, so they can stay open at all times. Browsers should be run under https rather than http (https is a higher security environment), and secure socket layer encryption is often advisable to ensure the security of the system being monitored. Even so, browsers are not as secure as VPNs. Browser connections can be hacked.

A VPN can open and close like a browser, but it has vast advantages in terms of network security. A VPN is a tunnel between the server being monitored and the server that is requesting its data. That tunnel is firewalled and encrypted. It is as good as gold for security. It takes extremely high skill levels to hack a VPN. The disadvantage of VPNs is that they utilize a fixed bandwidth. When a VPN connection is open, that amount of bandwidth is in use regardless of the number of cameras being monitored.

That bandwidth is no longer available for the business network connection to that site (Figure 17-13).

DIGITAL VIDEO

Cameras and Codecs

Digital video cameras are available in two types: digital cameras or analog cameras with digital codec converters. Digital cameras are an emerging trend. The predominance of cameras available are still analog, and to use them in a digital video system one must add a codec.

Digital cameras do not provide a baseband video output (PAL or NTSC). They are equipped with either a USB or Ethernet connection. They issue digital images directly.

A codec is a device that converts analog to digital. There are a variety of codec types, in the following categories:

Number of channels. Single-channel codecs support only one camera. Multiple-channel codecs support multiple cameras. Single-channel codecs are the best choice when the wiring infrastructure is predominantly digital, and multiple-channel codecs are a good choice when most of the wiring is analog. Multiple-channel

codecs facilitate wiring a number of cameras to a single point where perhaps an analog video switch used to be, its space now being occupied by codecs.

Number of video data streams. Many codecs output only one data stream per camera. Some support two, which is better. Each data stream can typically be configured to adjust the frame rate and resolution. With two data streams, you can adjust one for live viewing and the second for archiving. You might adjust the live viewing data stream at, for example, 15 frames per second (fps) and at medium resolution and the second stream at 4 fps and high resolution. Generally, it is desirable for archiving retrievals to display higher resolution than for live viewing, since you are looking for detail rather than just a transient image.

Audio/no audio. Some codecs support an audio channel and some do not. The audio channel will be its own separate data stream, usually under the same TCP/IP address.

Input and output contacts. Many codecs also provide one or more dry-contact inputs and outputs. These are useful to control nearby devices or to cause some activation in the system. For example, they could be used to unlock a door or to cause an alert if a door opens.

Compression schemes. Different codecs use different compression schemes, which are discussed later.

A basic digital image such as a BMP (bitmap) is composed of a large number of picture elements called pixels, with each pixel having its own data attributes. These images take up a lot of data space. It is common for a single BMP image to require several megabits of data. These large files are not useful for network transmission because they use too much network bandwidth. The images can be compressed (made into smaller packets) literally by throwing away useless data.

There are two major types of digital video compression schemes: JPEG and MPEG. JPEG (Joint Photographic Experts Group) is a scheme that results in a series of fixed images, strung together like a movie. MPEG (Moving Pictures Experts Group) is a similar group that from its inception created compression algorithms specifically meant for moving pictures.

- MPEG-1 was the earliest format and produced video CDs and MP3 audio.
- MPEG-2 is the standard on which digital television set-top boxes and DVDs are based. This is very high-quality video.
- MPEG-3 (MP3) is an audio codec.
- MPEG-4 is the standard for multimedia for the fixed and mobile Web.
- MPEG-7 and MPEG-21 also exist, but are for future projects.

Digital video security codecs and cameras are typically MJPEG (a series of JPEG images strung together as a stream of data) or MPEG-4.

BMP images are resolution dependent; that is, there is one piece of data for each separate pixel.

JPEG compression basically replicates similar data rather than storing it. For example, if there were a picture of a flag, the red portion might only be stored in a single pixel, but there will be a note to replicate the red pixel everywhere it existed in its original BMP file. This can achieve very high compression compared to BMP files.

MPEG compression takes this process one step further. For a sequence of images, the first one is stored as a JPEG image, and each subsequent image stores only the differences between itself and the previous image. The first frame is called an "I-frame," and subsequent frames are called "P-frames." When too much updating is occurring, the process stores a new I-frame and starts the process all over again. The MPEG protocol results in very efficient file compression.

Advantages and Disadvantages. Each JPEG image is a new fresh image. This is very useful where the frame rate must be very low, such as on an offshore oil platform with a very low bandwidth satellite uplink, or where only a dial-up modem connection is available for network connectivity. I used JPEG on an offshore platform with only a 64 kb/s satellite connection available. MPEG is most useful where there is adequate data bandwidth available for a fast-moving

image but where it is desirable to conserve network resources for future growth and for network stability.

DIGITAL RESOLUTION

Digital image resolution is the bugaboo of digital video. You can never have enough resolution. However, high resolution comes at a high price in network bandwidth usage and in hard disk storage space. There is always a trade-off between resolution and bandwidth/storage space. Thankfully, the cost of storage keeps dropping (I think we will soon see terabyte hard drives blister-packed for 99 cents), but I think that network bandwidth will always be a problem.

JPEG resolution is measured in pixels per inch (PPI). Proper resolution is required for good viewing. Ideally, you should be displaying one pixel of video image onto each pixel on the video monitor. If you display a JPEG image at a greater size on paper or screen than its native resolution, you will see a very fuzzy image (Figure 17-14). Common file sizes are from 120×160 to 720×480. Larger sizes are available with even higher resolution.

MPEG resolution is measured in Common Intermediate Format (CIF). In NTSC, CIF provides 352×240 pixels. In PAL, it provides 352×288 pixels. The lowest resolution MPEG image is a quarter CIF (QCIF) at 176×120 pixels, followed by CIF, 2CIF (704×240, NTSC), and (704×288, PAL), and finally 4CIF (704×480, NTSC) and (704×576, PAL). 16CIF will soon be available with very high resolution (1408×1152 for both formats), and there is also an amazingly low resolution SQCIF (128×96, NTSC). Most digital codecs provide CIF, 2CIF, and sometimes 4CIF resolutions (Figure 17-15).

FIGURE 17-14 Fuzzy JPG image.

FRAME RATES

To see moving images, they have to move. Frame rate is the rate at which one frame of video is replaced by another. The speed at which this occurs is measured in frames per second (fps). Some unique applications result in very slow frame rates of seconds per frame.

The human eye can visualize real-time motion as low as 12 or 13 fps. A minimum frame rate of 15 fps is recommended for real-time images. Many users prefer 30 fps because that is what is displayed on analog video. However, that frame rate is not required unless objects are moving rapidly.

Like resolution, frame rates affect both bandwidth and storage capacity in direct proportion to the fps.

DISPLAY ISSUES

Display Parity

Display parity is one of the problems that the security industry has not dealt with yet. This is achieved when the number of pixels sent to a screen is exactly the same as the number of pixels on the screen.

If one is displaying nine cameras in a window on a 20 in. LCD high-resolution screen, one might have only 160×120 pixels available on the screen for each image. Why would one want to send a 4CIF image (704×480) to that number of pixels? Why indeed? What happens to all those extra pixels? They are wasted, thrown away. The problem is that they are thrown away on the screen. They occupy tons (if that is a measure of screen processing) of central processing unit (CPU) and video card processing power before it gets thrown away on the LCD monitor.

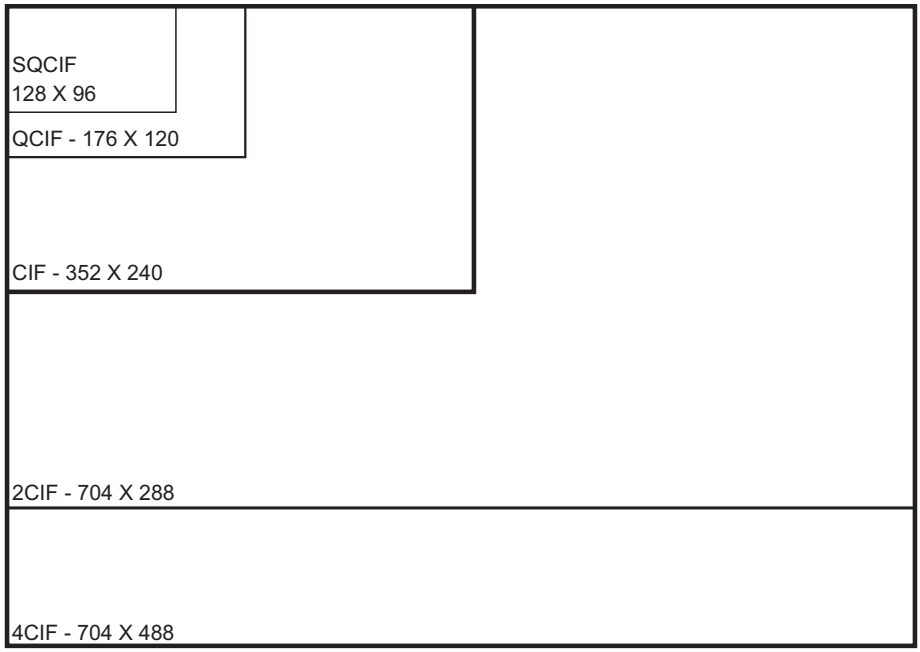


FIGURE 17-15 MPEG resolutions.

No problem you say? Who cares? You do, if you are smart. Here is the problem. A 4CIF image generates 337,920 pixels. Each individual pixel requires a great deal of CPU processing power and many more graphics processing units (GPUs). Both CPUs and GPUs are consumed for each pixel. The original supercomputer, the Cray-1 developed at Los Alamos National Laboratory in 1976, was capable of 80 megaflops of processing power. (Flops is a unit of CPU or video card processing effort; it is an abbreviation of floating point operations per second.) Although there is not a direct correlation between flops and pixel processing (there are approximately 40 variables involved in the calculation, making a calculation essentially meaningless), you can rely on the fact that it takes a lot of processing power to process video to the screen or to archive. At 30 fps, the computer is processing 10,137,600 pixels (10.1 megapixels) for each image at 30 fps. Remember, we were displaying 9 images. That calculates to 91.2 megapixels per second, and that is just for the video. You are also running the video application, and on larger systems you are also processing audio for the intercom, alarm/access control, and perhaps other data. One can easily exceed 100 megapixels being processed per screen on one's desktop. For 16 images, at 30 fps at 4CIF, the number exceeds 160 megapixels being processed in real time, and that is just on one screen. That will crash virtually any workstation regardless of processing power. High-resolution times high frame rate times many images can easily equal a computer crash. Additionally, pixels thrown away on the screen present a rough look to the images. Without a doubt, display parity results in the best appearance.

The ideal process here is to have software in the server that disposes of unneeded pixels before they are sent to the workstation. This approach of prerendering the video image has many advantages in quality of display and network throughput. However, to date, no software vendor that we know of is even thinking about this problem.

So what is a designer to do? Well, there are only three variables available to manage this problem: image resolution, frame rate, and processing power.

First, there is little need to display images at 4CIF or greater unless one is displaying at full screen. It is better to send live images to the screen at 2CIF because the extra pixels will just be thrown away and no good will be served by the extra resolution that is consuming unneeded network bandwidth and processing power.

Second, archived images do not usually need to be displayed at 15 or 30 fps. Use a slower speed and higher resolution for archived video. When one calls up archived video, one is usually interested in seeing as much detail in the image as possible. Use higher resolution and lower frame rate. There are a few applications in which this is not appropriate, such as for casino environments, where fast-moving hands hold the secret to cheating.

Finally, I usually design systems with lots of processing power, typically dual Xeon™ computers as workstations. Dualcore processors better that. Expected advances will put teraflops of graphics processing power at hand.

Storage Issues

As with display, storage consumes lots of data and processing power. Unless there is a compelling reason otherwise, it is best to store data at a slower frame rate than for live viewing. This not only saves disk and tape space but also helps ensure growth capacity.

MANAGING DATA SYSTEMS THROUGHPUT

Network throughput management requires math, sometimes lots of math, but it is a good investment. I do not recommend running any network or network segment beyond 45% of its rated capacity. If there is a segment that has a capacity of 100 Mbps, keep traffic to 45 Mbps. If it is a gigabit backhaul segment, keep the traffic to 450 Mbps. If you have to exceed 450 Mbps, it is better to use multiple gigabit communications paths or a 10 GB path. Your client will not likely understand, but he or she will not sue you either.

There are two ways of managing network throughput: more capacity and network segmentation. The cost/benefit is usually in favor of network segmentation.

By segmenting the network into subnets or VLANs, one can manage the traffic to manageable levels. All traffic does not have to be everywhere. By recording video remotely rather than centrally, traffic is diminished. If a backup is needed, or if there is a concern about the loss of data in remote storage, centralized recording is possible at far greater cost in network traffic and infrastructure cost. An alternative is "neighborhood" archiving, where a few sites are gathered together for storage, limiting traffic on the enterprise network.

SYSTEM ARCHITECTURE

Servers

Servers provide the guidance and direction for the entire system and store its activities and history. A server can operate several applications simultaneously, and a server equipped with a dual-core CPU can also prioritize those services, ensuring that, for example, intercom calls always go through. Servers provide several basic services.

Directory Service

The directory service provides the routing information to locate cameras, intercoms, and archived video on demand. It also maintains the necessary information for all system devices to communicate effectively.

Directory services can be local or global. In an enterprise integrated security system, the directory service may be both, with a global directory service centrally controlled, and local servers may maintain their own subordinate automatic fail-over directory services in case of loss of communications with the global directory server.

Enterprise integrated security systems also typically use an automatic fail-over server that runs parallel to the main server but in another

location, ready to take over its activities immediately upon a failure of the main server.

Archiving Data

The server will typically archive alarm/access control, video, and intercom activity, indexing it by date and time and often correlating video and voice data to alarm and security events so that the operator has immediate access to appropriate video and voice as he or she views alarm activity. Enterprise systems also typically use an automatic fail-over archive server.

Remote Access Services

Web Access. A VPN helps ensure data integrity for off-site Web service connections. Remote access from within the domain is often accommodated by use of a VLAN.

E-mail and Pager Notification Service. The server software may support e-mail and pager notification. These will require exchange server or similar software or a dial-up or Web connection for a pager.

Hardware Configurations

CPUs. Generally, it is appropriate to specify the fastest or nearly fastest CPU available for the server with significant cache memory and a very fast front side buss.

Memory. More is better. At least 2 GB of RAM should be considered in 2007 era terms. As this book ages, more memory should be considered. Fill the thing to capacity. You will not regret it, and memory is almost cheaper than candy bars.

Disk Storage

Operating Systems and Programs. All system servers should be equipped with multiple disks, including two mirrored automatic fail-over drives for operating systems and programs, complete with current configurations. These should be kept up to date so if one fails, the other takes over immediately. This is also less expensive than a full hot redundant off-site fail-over server and should be done even when a redundant server is used.

Additional disk slots should be dedicated to data archive up to the server's capacity. Disks are so inexpensive that it is almost always appropriate to specify the largest disks available. RAID-5 should be considered and configured to 500 GB segments for rapid searching of archived data.

Where additional disk capacity is necessary, external storage capacity should be considered. There are two methods of external storage.

Tape or Disk. External storage is available in both tape and disk. It is generally recommended to use both. Disks can store up to a given time depth. Beyond that, you can store endlessly on tape. For very large storage requirements, a tape carousel automatically handles the process of keeping fresh tapes loaded and used tapes stored and ready for use. The carousel can be expanded to store as much or as little as is appropriate based on network archive usage and the length of time storage is desired.

Network Attached Storage. Network attached storage is external storage that is attached directly to the server switch. This is the least expensive option, but it has a negative effect on network throughput. Accordingly, I do not recommend NAS.

Storage Area Network. A SAN is a separate network on the backside of the server that is dedicated only to moving storage data between servers and the external storage media. There is a perception that SANs are unnecessarily expensive, but this does not have to be the case. A SAN can be created simply by placing an additional NIC in the server and porting archive data out the back to the external storage. Where multiple servers or multiple external storage units are required, a SAN switch handles the task. SANs make the best use of the primary data network over which live data are flowing. They place virtually no additional burden on the live data network, conserving its spare capacity for system growth. SANs are always recommended for external storage, even if there is only one server and one external storage unit.

Workstations

A workstation is a computer used by a person who operates the system. There are a variety of basic workstation types.

Security Monitoring (Command) Workstations. Security command workstations are used in security command centers, typically in enterprise security systems. A security command center typically includes two or more security command workstations and may include an array of large-screen video monitors to support the joint viewing of images by operators at several consoles. These workstations typically include alarm/access control/digital video and security intercoms as well as report writing programs.

Guard or Lobby Desk Workstations. A guard or lobby desk workstation is a single computer dedicated to supporting a guard's desk duties in a lobby. These may include alarm/access control, digital video, and intercom.

Administrative Workstations. An administrative workstation supports management of an integrated security system, including system configuration, database management, and reports.

Photo ID Workstations. Photo ID workstations are used to create identification badges for use with the access control system. A photo ID workstation typically includes a camera, backdrop, light source, sitting chair, digital camera, and workstation and may include a posing monitor to help the subject pose to his or her satisfaction. On larger systems, there may be several photo ID workstations in a single area.

Access Verification Workstations. On high-security installations, an access verification workstation may be used in conjunction with a man-trap and card reader to ensure that the person passing into a secure area is indeed who he or she claims to be and that his or her credential is valid for the secure area. The access verification workstation displays a photo of the cardholder each time a card is presented. This allows a guard at the workstation to verify that the face is that of the valid cardholder.

Edge Devices

Edge devices include cameras, intercoms, card readers, alarm detection devices, electrified door locks, and request-to-exit detectors. These are the devices that interface with the user. On a typical integrated security system, the edge device connects with a data controller or codec, which converts its native signal (audio/video, dry contact, or data) to a uniform TCP/IP standard. Thus, controllers and codecs are also edge devices. The edge devices typically connect to the system through a data switch.

Infrastructure Devices

Between edge devices and servers/workstations is the digital infrastructure, which connects the system together and manages its communications rules.

Switches

Digital switches are the connection points for almost all system devices. A digital switch is a device that not only provides a connection point but also can manage how each device communicates with the system. A digital switch is like a mail carrier on a mail route, who ensures that each house gets the mail that is addressed to it.

Switches can segregate communications between devices and manage the priority and limit the bandwidth of the data of different devices. Switches generally have a number of RJ-45 eight-conductor modular jacks (typically 8–48) and can cascade communications in a ring or tree architecture. The switch must be specified to support the amount of data that is expected to go into its edge ports and out of its infrastructure ports. It is wise not to exceed more than 45% of the rated capacity of any switch for all signals combined, under worst-case conditions. Switches are OSI layer 2 devices, but better switches can also perform OSI layer 3 management functions. These are commonly called "managed" switches. Switches should

be able to support IGMP querying and IGMP snooping in order to support video multicast. Ample memory is recommended (at least 100 KB per port), and the switch should be able to support VLAN operation. If the switch may need to become part of a trunk within a VLAN, then it should also be able to support 802.1Q protocol. For outdoor operation, a robust environmental tolerance is needed. The switch should be able to operate from well below freezing (–10°F/–23°C) to high temperatures (160°F/70°C is ideal). These are commonly called "hardened" switches. Redundant power supplies are also recommended.

Routers

Routers manage data traffic at a more global level, and are OSI level 3 devices. An edge router is like a local post office that routes mail from one locale to another, where it will be handed off to the neighborhood postal worker (the switch). A router that manages traffic for an entire organization to the Internet is called a core router.

Routers are capable of segregating traffic into subnets and VLANs, creating logical separations of data and making communications within the network much more efficient and secure.

Firewalls

A network firewall is a computing device that is designed to prevent communications from and to some devices in support of an organization's network security policy.

Wireless Nodes

Wireless nodes are radio frequency transceivers that support network communications. Often, they also incorporate network switches, and sometimes they can incorporate routers and even firewalls. They also commonly encrypt data placed on the wireless link.

Network Communications Speeds

There are four common speeds of network communications:

- 10Base-T: 10 Mbps
- 100Base-T: 100 Mbps
- 1000Base-T: 1 Gbps
- 10,000Base-T: 10 Gbps

Cabling

Network cabling can be wired or fiber optic. Fiber optic cabling types include single mode and multimode.

Wired Cabling. Category 5e and 6 cables are used for network cabling. Both have a native distance limit of 300 ft. Cat5e and Cat6 cables can support 10Base-T, 100Base-T, and 1000Base-T connections, with distance decreasing as the speed increases.

Fiber Optic. Fiber optic cabling can support faster speeds, longer distances, and simultaneous communications. Unlike wired cable, fiber only supports a single communication on a single frequency at one time.

Multimode. Multimode fiber uses inexpensive LEDs operating at 850 or 1500 nm to transmit data. Multimode fiber is made of inexpensive plastic. In multimode fiber, the light propagates through the fiber core, bouncing off its edges (thus multimode). Multimode fiber can support only one communication at a time on each frequency. Typically, two fibers are used together, one to transmit and one to receive.

Single Mode. Single-mode fiber uses more expensive lasers and optical glass. Single-mode communication is right down the center of the glass fiber, never bouncing (thus single mode). Single-mode fiber can stand higher power and thus yields longer distances.

Scaling Designs

Systems can be scaled by creating subnets, which can segregate the system based on function or location. This approach allows the master system

to have oversight and observation of the activities of all of its subsystems while not allowing the subsystems to see or affect each other.

INTERFACING TO OTHER ENTERPRISE INFORMATION TECHNOLOGY SYSTEMS

Enterprise LAN or Wide Area Network

The fundamental interface of the integrated security system is to the organization's enterprise LAN or wide area network (WAN). The recommended interface is to configure the enterprise security system as a VLAN on the enterprise LAN/WAN.

Remote monitoring from inside the enterprise LAN can be accomplished by placing the monitoring computer on the VLAN. If the monitoring computer must also be used on the business network, it should be equipped with two NICs to better segregate the VLAN from the LAN.

Remote monitoring over the Internet should be accomplished by use of a VPN.

Process Control Networks

Integrated security systems are classified as process control networks. A process control network differs from a business network in that it is a closed network, dedicated to a special purpose, and is segregated from the business network. The integrated security system may integrate with other types of process control networks, including building automation systems, elevators, telephony systems, fire alarm systems, parking management systems, and vending systems.

Building Automation Systems. Building automation systems (BASs) include controls for HVAC, lighting, signage and irrigation control, and the control of other building systems. BASs may interface to the integrated security system via RS-232 or TCP/IP. The common interface language is ASCII delimited files, although sometimes database integration is possible.

Elevators/Lifts. There is often good reason to integrate security systems with the elevator system of a building. This interface permits the control of who goes to what floor on which elevator at what time. Additionally, it is common to place video cameras and intercoms within elevators.

There are two basic types of elevators: traction and hydraulic. Traction elevators are used in high-rise buildings, and hydraulic elevators are commonly used in low-rise buildings and parking structures.

Access Control Interfaces. There are two common types of elevator access control interfaces: floor-by-floor control and hall call control. Hall call control simply enables or disables the hall call pushbuttons in the elevator lobby. Floor-by-floor control allows control over the selection of individual floors in each car for each cardholder. Floor-by-floor control components include a card reader in the elevator and an access control system controller that enables or disables each floor select button based on the authorizations for the individual card presented to the reader in the car.

More sophisticated floor-by-floor access control systems provide an indication of which floors the card can select by turning off the button lights to floor select buttons for which the cardholder is not valid and may also keep a record of which floor was actually selected. Today, those functions are handled in the programming of the elevator controller. For older elevators, as was done in the past, those functions can be accomplished with elegant relay logic programming.

Elevator control mechanisms affect the design of the elevator access control system. There are three common types: automated, relay, and on-the-car control. These are covered in detail elsewhere in this book.

Video cameras can be interfaced up the hoistway by using coax, ribbon cable, laser, or radio frequency methods.

Intercoms can be the direct ring-down type or dedicated intercom type. They must ring to a location that will always be answered and must never be unmanned, even for a few minutes.

Private Automatic Branch Exchange Interfaces. Private automatic branch exchange (PABX)

systems facilitate the connection of a number of analog or digital station sets to a central switch. The PABX switch will accommodate a number of central office telephone lines (from a couple to hundreds) and a number of telephone station sets (from six to thousands). The PABX switch routes incoming calls to the correct extension and routes outgoing calls to an available central office line.

Additional features of PABX switches may include direct inward dialing so that certain extensions can be dialed directly from the outside without going through the switch, an automated attendant, call waiting, voice mail, and many other unique features. Internal intercom functions are usually standard.

Station sets may be simple or complicated. Simple station sets may look like a home phone, whereas more complicated sets may display time/date and incoming caller ID. The set also may have many speed-dial buttons and may also show the line status of frequently called internal numbers. An operator's station set may display the status of every extension in the system by a field of lamps and select buttons or in software.

PABX systems are normally controlled by a dedicated computer located in the main telephone closet. They are capable of sophisticated interfaces to other systems, including security systems.

The security designer can use the PABX system as a security intercom system by utilizing door stations in lieu of standard station sets (depending on the manufacturer and model of the PABX system).

For almost every installation, it is important for the security console to be equipped with a direct central office telephone that is not routed through the PABX switch. This serves as an emergency communication link in case of total power or equipment failure.

Voice Over IP Systems. PABX switch systems are rapidly being replaced by Voice over IP (VoIP) systems. VoIP systems do not rely on central office telephone lines for their connection to the telephone company. Rather, they utilize the Internet for that connection.

The telephone station sets may be either conventional station sets with a VoIP converter or network devices.

VoIP phone systems are extremely flexible since all of their functions operate in software. However, they suffer from two major potential problems relating to the security of the organization they serve. VoIP systems are subject to Internet outages, which are much more common than central office line outages that operate on battery power from the central office. With central office lines, if electrical power fails, it is likely that the telephone lines will still work. This is not the case with VoIP phones. Additionally, VoIP phone systems are subject to intrusion by skilled hackers, making communications on a VoIP phone extremely unsecure.

VoIP phones are a natural for integration with other systems, although those interfaces have yet to be developed by the industry.

VoIP systems should easily accommodate integration with IP-based security intercoms and with pagers. Digital two-way radios are also a natural point of integration.

Fire Alarm Systems. Fire alarm systems are among the oldest of process control networks used in commercial buildings. These typically have their own proprietary infrastructure that may be unique to the manufacturer. However, they often interface to other systems by means of RS-232 serial data streams or TCP/IP Ethernet. Typically, the interface is an ASCII delimited data stream that identifies the change of state of a fire alarm zone. Occasionally, a designer may see access to a database that displays real-time status of all points in the system.

Public Address Systems. Public address systems can be configured with an analog or a digital infrastructure. The interface to a public address system will always be a one-way audio signal from the security system to the public address system for paging purposes.

Typically, the interface between the systems includes an audio signal and a zone selection, plus a push-to-talk momentary trigger. The interface may be analog or digital. Typically, analog interfaces are used on smaller public

address systems, and larger systems may receive an analog or a digital interface for the audio stream.

Analog interfaces employ a microphone or line level input to the paging system and one or more dry-contact inputs to select one or more zones. Often, it is possible to select groups of zones or an "All Call" selection, in which all zones will be paged.

Digital interfaces employ a digitized audio feed and a data string that performs the zone selection. On larger systems, both analog and digital, multiple public address amplifiers may be used to support different areas of a building or different buildings on a campus. In such cases, the zone selections employ a hierarchical zone selection, in which one string may select the building, another selects the amplifier, and still another selects the zone on the amplifier.

We have also used the alarm/access control system to perform zone selections, controlling a single audio buss. This is an effective way to make a simple public address system operate like a very expensive one.

Parking Control Systems. Parking control systems perform a number of functions:

- Allow vehicles into a parking structure (car park) or parking lot.
- Direct cars within a parking structure to one area or another.
- Meter the number of cars in the structure.
- Display up/down count signage of available spaces to drivers of cars entering.
- Produce tickets for cash transactions.
- Read the tickets and facilitate cash transactions for parking.
- Use buried vehicle-sensing loops to verify the presence of a car at a card reader or in the path of a barrier gate, or to notify the gate that it can close after a car has passed through.
- Access control systems interface with parking systems to facilitate the entry of cars to the parking area.
- Access control readers may simply provide a dry-contact closure to notify the gate to open.

The parking system may also feed back a dry-contact signal that causes the card reader to refuse to read cards if the parking area is full. Access control card readers may be short range (6 in.) or long range (3 ft), or they may be overhead vehicle tag readers that do not require the driver to roll down the window.

The access control system may also be integrated with the parking monthly cash control system such that the card is enabled or disabled based on payment of a monthly fee. The card readers may also permit special privileged parking for handicapped people, expectant mothers, high-rent tenants, high-level executives, and so forth.

Vending Access Management Systems. Vending access management systems are a variation of access control systems that are interfaced with a product vending system to provide product in kind for a prepayment or a charge account. In effect, the access control system is used like a credit or debit card.

Vending systems may include fuel management and vending machines, or the card may be used at a school bookstore, and so forth. This requires a database interface between the access control system and the vending system such that the vending system has daily status on the validity of the card and it keeps a running database of credits and debits.

More Protocol Factors

Wired and wireless digital security systems both use unicast and multicast protocols to communicate. Unicast protocols, commonly TCP/IP, are meant to communicate a signal from one device to another device. They ensure that the communication occurs by verifying the receipt of every packet of data. Unicast protocol is commonly used for pure data, such as alarm and access control data. Most networks are inherently based on TCP/IP protocol.

Multicast protocols such as UDP/IP and RTP/IP are used to broadcast data to any number of receiving devices. Unlike unicast TCP data, if a packet is not received, there is no mechanism or

attempt to verify that and resend the packet. Multicast is widely used for video and audio data.

Do not confuse multicast protocol with multipath. Multipath is the phenomenon caused by radio frequency reflections, and multicast is the distribution of a single digital signal to more than one destination using a single signal to which each receiving device signs up on a subscription.

Multicast can both reduce and increase network traffic, depending on how the network is configured. Multicast can reduce network traffic because there is no attempt to resend data. It is sent only once. Especially for radio frequency and satellite systems, where latency (circuit delays) can be a factor, the receiving computer can make many requests for unreceived packets. This has the effect of increasing data traffic for no good purpose because the video frame or audio signal cannot be received in time to be useful, since it has already been displayed or heard.

However, because multicast transmits to any device that will listen, it is important to configure the network to adapt to multicast protocol so that devices that do not need to process the data will not hear it. Otherwise, many devices are kept busy trying to process data that is of no use to them. On security systems, some devices have a capability of only 10Base-T (10 Mbps). Their input can be swamped by the signals of only a few video cameras, rendering them incapable of communicating. The effect is similar to a denial-of-service attack on a Web site, where it is flooded with unwanted traffic, bringing it down.

It is important to understand that multicast was designed for an entirely different application than to support distributed video cameras. It was designed to support a single source transmitting data to many destination devices. In video systems, there are many sources (cameras and intercoms) transmitting to a few destination devices (servers and workstations). This difference can have unintended consequences for the uninitiated. For example, in conventional multicast environments, the "edge" switches (those at the outermost devices) do not have to be managed switches. However, in distributed digital video systems, the outermost switches should be managed, because when multicast touches a device that cannot handle multicast protocol, that device broadcasts a return message for each packet it sees, often bringing down the entire network. When managed edge switches are used, however, each individual port can be set up with IGMP snooping to prevent multicast signals from getting to unicast devices (e.g., alarm/access control system panels).

Multicast Anomalies. Additionally, be advised that multicast traffic can have unanticipated side effects even on systems that are properly configured for it. For example, adding a set of mirrored backup archive servers to a security system requires the system to operate in multicast mode since both the primary and the backup servers are receiving the data of all digital cameras at all times. On a typically configured digital video system, this can result in directing 200 Mbps of data traffic across the backhaul network to the backup servers. It is a little known fact that multicast data traffic can have an adverse effect on intercom codecs. I was once confronted with an enterprise security system that exhibited audio distortion in its intercoms when the backup servers were turned on. The additional data traffic was enough to cause the intercom talk codecs to distort the audio only when the archive servers were turned on (changing the system from unicast to multicast for all video signals). By reducing the volume setting of the talk intercoms, the "clipping" of audio signals was eliminated. This condition is especially obvious where audio converters are used to convert two-wire intercoms to four-wire for use with conventional audio codecs, because the two-/four-wire converter also inserts an additional volume control in series in the circuit.

Multicast is a very "user surly" environment. It is especially not friendly to radio traffic and should not be used on such by the unsophisticated designer. Many configuration settings are required to operate multicast on a wireless mesh network to ensure that the radios do not retransmit the multicast traffic endlessly, thus flooding the mesh with unnecessary traffic.

It is ideal to configure the digital video network into two distinct VLANs, where VLAN1 is the camera-to-server network and VLAN2 is the server-to-workstation network. Run VLAN1 (the cameras) in unicast and VLAN2 (clients) in multicast. Configure IGMP querying on a primary and backup core switch, and configure all switches to support IGMP snooping to ensure that no unicast devices retransmit multicast signals. IGMP querying asks which switch ports want to sign up for multicast signals, and IGMP snooping sends those signals only to those ports. Utilize managed switches to ensure IGMP conformance.

SUMMARY

Understanding information technology infrastructure is the basis for a successful integrated security system design. The reader should carefully read and understand this chapter in order to succeed as a designer.

The TCP/IP suite of protocols is the basis for information technology networked systems. This chapter provides a detailed description of how TCP/IP works. The designer will not achieve success without a comprehensive understanding of TCP/IP.

TCP/IP operates on levels 3 and 4 of the OSI networking model. Data is encapsulated from the application program through the seven layers down to the network wire, sent across the network, and then decapsulated back up the seven layers to the application on the other end.

TCP protocol is able to fix bad communications. Other protocols in the TCP/IP family include UDP and RTP, which do not fix bad communications but are better suited for streaming data, such as video and audio.

TCP/IP is also an addressing scheme. Each network connected device is assigned a TCP/IP address that identifies its location on the network. Addresses can be assigned automatically or manually.

Common wiring schemes include Ethernet and fiber optic cables. Ethernet is available on Cat5, Cat5E, and Cat6 cable at speeds of 10, 100, and 1000 Mbps or 10Base-T, 100Base-T, or 1000Base-T (gigabit Ethernet). Fiber optic runs can be on either single-mode or multimode fiber. Single-mode fiber can carry more data farther. Multimode cable and transducers are less expensive. Gigabit switches are often available with fiber connectors to link switches together over long distances, and RJ-45 connectors are used for short runs of Ethernet cables to local devices.

Edge devices include IP video cameras, IP intercoms, and codecs. Network infrastructure and wiring is connected using hubs, switches, routers, and firewalls. Hubs are rarely used today because they simply connect wires together and do nothing to handle network contention. Switches handle the connection of local devices. Routers control where network communications can go. Firewalls exclude unauthorized devices from gaining access to the network. Intrusion detection systems monitor the network firewall to detect any attempt to intrude into the network.

Integrated security system network computers include servers and workstations. Servers can include directory service servers (Windows directory service), Internet information services, domain name service, and other network management services. Other services may include archiving, application program service, ftp, http, e-mail, and broadcast services. Workstations provide the interface between users and the network. Printers and mass storage systems round out the network attached devices. Mass storage systems include NAS and SANs.

Network architecture includes simple networks, LANs, and WANs. Advanced network architecture includes backhaul networks, subnets, and VLANs. Network connection types include peer-to-peer and client/server configurations. Systems can be monitored remotely and safely using browser (http) or VPNs. Digital cameras can link directly to the network, whereas analog video cameras require a codec interface.

Typical video compression schemes include MJPEG, MPEG-2, and MPEG-4. MJPEG is a stream of individual images strung together to show movement, whereas MPEG schemes

display a single image and then update subsequent frames only with the changes in the image.

Workstation types include security monitoring centers, guard or lobby desk workstations, administrative workstations, photo ID workstations, and access verification workstations.

Integrated security systems can interface to many other types of systems, including process control networks, BASs, elevators, PABXs, VoIP systems, fire alarm systems, public address systems, parking control systems, and vending systems.

Multicast protocol is sometimes used in digital video systems, but it is fraught with many nuances requiring special skills and knowledge. I recommend a thorough understanding before implementing multicast protocol.

CHAPTER

18

Security Officers and Equipment Monitoring

Scott Fishman

INTRODUCTION

After basic training, a security officer will be assigned a specific post. Each post requires additional training, and that training starts with post orders. Post orders are written procedures on how a security guard is to perform his or her duties throughout the shift. Once written, policy, post orders, or procedures will be reviewed and approved by upper management of the organization. These policies tend to remain in place for a period of time, but the post orders/procedures need to be reviewed every six months. This is because procedures for carrying out the policy are subject to change to meet the changing demands of the business unit. Post orders are usually kept in both soft copy and hard copy for easy access.

Post orders should contain at least the following information:

1. Date of revision
2. What is confidentiality
3. Instructions on how to deal with public relations
4. Security staffing levels, hours of coverage, and specific functions and duties
5. Description of the building (floor plans if possible)
6. Specific instructions on handling of emergency situations
7. Emergency contact information including after-hours contact information
8. Code of ethics and standards of conduct

Security personnel should first be trained in the basic areas:

1. Security policy and procedure
2. Professionalism
3. Authority of a security officer
4. Relationships with law enforcement
5. Patrol procedures
6. Observation techniques
7. Challenging techniques
8. Investigations
9. Report writing
10. Emergency medical assistance, first aid, and the AED units
11. Workplace violence
12. Operation of security equipment

One very important post for security is the command center. This is a center from which the security staff can view, record, and retrieve video from surveillance cameras, also known as closed-caption television (CCTV). A command center should have a minimum of two security officers, who may be called command center operators or CCTV operators. A security office can be managed by one security guard. The center is a place where security officers can view images of video

surveillance from hundreds or even thousands of cameras.

Something that always needs to be watched is the length of time the guard is viewing the CCTV. Periodic breaks are very important as the human body can only view something for so long before the eyes start to become tired. The ideal setup for a moderately sized center is two security guards. Each officer monitors the CCTV for one hour and then they switch the monitoring responsibilities. This way there are always fresh eyes viewing the cameras.

The most important task for a command center operator is to uphold safety of staff members and the public and prevent any crime. One may joke that the only requirement to work as a command center operator is that you have unblinking eyes, but there are in fact many skills and traits that come in handy.

COMMAND CENTER

It is imperative for command center operators to have extraordinary attention to detail since they will be watching live pictures on an entire bank of monitors. Command center operators work in a central control room watching up to 15 screens at a time, receiving live feeds from more than 100 surveillance cameras. It is extremely important that every activity be closely observed to maintain safety and order. Shifts are scheduled tightly to make sure that there is no downtime during shift changes. Some command center operators work alone, while others work in teams. Command center operators have specific procedures to follow if they witness any illegal or suspicious activity and may often call or radio security staff or police.

To work successfully as a command center operator it is important to have some specific skills. Two of the most important traits, of course, is excellent eyesight and attention to detail. It is also important to be able to react quickly in case of an emergency and be discreet. Discretion is important because operators must not ever relay what they have seen on the monitors to the public. Their ability to work unsupervised is also important since they are responsible for watching a lot of screens at once and then need to be able to make quick judgment calls about what they see.

Command center operators can operate the cameras from inside the control room, which can help them prioritize what they are watching. Certain areas may be more important to watch during certain times or in case of emergencies. For instance, if an alarm goes off in a building forcing security to check into the problem, the command center operator will monitor the area and communicate with security if he or she sees anything suspicious.

Command center operators are often in contact with other security staff and the police to report crimes such as theft and vandalism. Because command center operators can see what is happening live they are often able to aid in the capture of criminals before they leave the scene of the crime. In addition to the task of monitoring live footage, command center operators are responsible for maintaining the video recordings. All recordings are kept for a specific amount of time in case the police need them for an investigation. They must also keep a written log of all incidents they witness in case the police require that information as well.

The best practice for CCTV is to have a digital video system. The most commonly used are DVRs (digital video recorders). These have the ability to record and play back the images that the CCTV captured. Through the DVR network a command center operator can view other locations that are not local.

There are two types of cameras used by security departments: fixed cameras (static—they do not move) and PTZ (pan, tilt, and zoom). A fixed focal or variofocal lens is used with the camera to capture a defined field of view. A benefit associated with using a fixed camera is that the camera is always aimed at the desired view, which facilitates assessment. A PTZ camera is able to pan (move side to side) or tilt (move up and down). This is to help the operator to observe/access a much larger viewing area. Plus these cameras are available in HD, as are the monitors.

FIGURE 18-1 Command center.

The use of CCTV is only one element to a company's security plans, and CCTV can be installed for a small cost compared to adding security staff to cover its function. One or two security officers are able to watch many locations from one central location, meaning that these security officers can view and respond to a location by means of watching the CCTV from another building. They are also able to view the CCTV playback from another location, in case there is an incident that takes place and they are at another location and need to provide the police with video. The use of CCTV equipment is one way that a company can save money with the reduction of the security guard staff, which considerably lowers the cost of security.

BEST LOCATIONS FOR CCTV

Entrance and exit doors present your best chance of viewing and recording facial images that can be used for identification purposes. To capture a useful ID image, the security camera should be set to view an area of about three feet wide; that's the width of the average door. Caution should be used when pointing cameras toward exterior doors. As the door opens, a sudden change in light will often cause the subject to go black. Instead of the facial image being captured, there will be nothing but a dark outline. In many cases the guard will have an easier time viewing an exit. The lighting will be more even since the security camera will be facing away from outside light. The design and scope of the physical assets protection management system is based on the size, nature, and complexity of the organization and site.

Targets

Targets include cash drawers, jewelry cabinets, safes, filing cabinets, or any area that a thief may target, as well as areas that may be considered *high risk*. In these areas, security cameras should be set up to capture as wide an image as possible. The idea here is not so much to identify a face as it is to review or respond to a crime. These are also areas where security cameras may be mounted relatively high so that they can see down into cabinets and drawers.

Secluded Areas

Parking lots and back alleys are also good locations for security cameras. The images captured in these areas are useful for investigating vandalism or violence. The deterrent value of a camera system also comes into play in these applications. Seeing a security camera staring at them, potential

perpetrators may think twice about committing a criminal act. As part of the physical assets protection management system plan, guards should review the exterior light level (see Chapter 9).

Testing and Maintenance

I recently read in a security text to make sure exterior doors that have a portable alarm are tested annually. To my surprise, when we checked at our location, every battery was dead. My point is, *develop a maintenance program that includes all physical asset protection devices*, and in the maintenance program, require vendors to supply only qualified technicians.

INTRODUCTION TO ACCESS CONTROL AND BIOMETRICS

Perimeter barriers, intrusion-detection devices, and protective lighting provide physical-security safeguards; however, they alone are not enough. An access control system must be established and maintained to preclude unauthorized entry. Effective access control procedures prevent the introduction of harmful devices and components. They minimize the misappropriation, pilferage, or compromise of recorded information by controlling packages, materiel, and property movement. Access control rosters, personal recognition, ID cards, badge-exchange procedures, and personnel escorts all contribute to an effective access control system.

DESIGNATED RESTRICTED AREAS

The security manager is responsible for designating and establishing restricted areas. A restricted area is any area that is subject to special restrictions or controls for security reasons. This does not include areas over which aircraft flight is restricted.

Restricted areas may be established for the following reasons*:

- The enforcement of security measures and the exclusion of unauthorized personnel.
- Intensified controls in areas requiring special protection.
- The protection of classified information or critical equipment or materials.

Access control and biometrics will grant or deny admittance and ensure authorized access. Badges not used in 30 days must be deleted. These devices increase the level of protection with a high degree of reliability.

SUMMARY

The functions of a physical assets protection management system are to deter the occurrence of an undesirable event, delay an adversary from reaching his or her target/assets, detect an undesirable event or adversary attack, deny an adversary from reaching his or her target, and enable law enforcement/security to successfully respond to an undesirable event.

*This information is from Joseph Nelson, CPP, author of Chapter 15 of this book.

CHAPTER

19

Glass and Windows

Lawrence J. Fennelly, CPO, CSS, HLS III

INTRODUCTION

The purposes of windows, aside from aesthetics, are to let in sunlight, allow visibility, and provide ventilation. When you research the types of windows and glass available you start to see terms like *weather ability, durability, thermal performance*, *triple-insulating glass*, *thermal barriers,* and *solar windows*. Every day another building is going "green," such as by diffusing light that enters a building, which cuts down on cooling costs, and the technology goes on and on from there.

"Healthy" buildings using current and innovative technology are contributing to healthier people, through the use of proper cleaning chemicals and green cleaning. All of this creates a better environment and reduced energy costs.

TYPES OF GLASS

There are five main types of glass: laminated, sheet, tempered, bullet-resistant, and float:

Laminated glass. This is a type of safety glass that contains polyvinyl butyral (PYB) or a similar substance and therefore holds together when shattered. It comes in high-performance laminated glass for structurally efficient glazing.

Sheet glass. Least expensive and most vulnerable to breakage, with a thickness of typically 3–4 mm.

Float glass/annealed glass. Has the quality of plate glass combined with the lower production cost associated with sheet glass manufacturing, and is virtually distortion and defect free.

Tempered glass. Treated to resist breakage and is three to five times stronger than sheet glass, because it is 10 mm tempered.

Bullet-resistant glass. Constructed using a strong, transparent material such as polycarbonate thermoplastic or by using layers of laminated glass. The polycarbonate layer is often sandwiched between layers of regular glass, and since the glass is harder than the plastic, the bullet is flattened and prevents penetration. It can be designed for both bullet and blast resistance. It will let in light and keep out trouble.

GLASS AND SECURITY

Take, for example, a police department recommends to a company that for tighter security a glass wall and counter need to be added to create a barrier between the general public and the receptionist. In addition, a glass door is also installed that works off an access control, and

if a visitor needs access, he or she would be escorted inside by a personnel member. Some people might not like this inconvenience, but it is the trade-off for security.

The following are factors to be considered for the selection of the type and size of a window:

- Energy efficiency and quality of unit
- Amount of sunlight, ventilation, and visibility
- Material and desired finish:
  - Wood
  - Metal, aluminum, stainless steel
  - Finish color and "green" products

Window hardware should have durability, function, and lock fitting. Consider the following:

- Type of glazing available for effectiveness of weather-stripping and wind pressure, explosion blasts, and fire
- The size and shape to prevent access, and the cost to replace if vandalized
- The use of grills or bars inside or outside
- There are three types of glass:
  1. Plate glass
  2. Sheet glass
  3. Float glass

In addition, the following are other considerations to keep in mind:

- Whether to use tempered glass, laminated glass, wired glass, bullet-resistant glass, and plastic glazing (e.g., polycarbonate or acrylic)
- Visibility requirements
- The thickness; by altering thickness and composition, such as adding layers of glass or polycarbonate, security glass laminates can be customized to meet your requirements for specific risks/threats
- The solution to security problems are to identify risk factors through assessment, use laminated glass with a thicker vinyl interior layer, and use compression operating window frames, awnings, and casements
- Float glass can be broken with an average rock and toughened glass will shatter when it breaks
- A crowbar can break or destroy standard window frames
- Standard laminated glass (6.38 mm thick) can be broken with several blows from a hammer[2]
- Energy savings
- Hardware, such as glass door hinges, locks, sliding glass door systems, and clamp supports, are available online or at any hardware store.
  - Sliding glass doors should be installed so as to prevent the lifting and removal of the glass door from the frame from the exterior of the building
  - Fixed panel glass door (nonsliding) should be installed so that the securing hardware cannot be removed or circumvented from the exterior of the building
  - Each sliding panel should have a secondary locking or securing device in addition to the original lock built into the panel. The secondary device should consist of:
    - Charlie bar–type device, secondary locking device
    - Track lock, wooden or metal dowel
    - Inside removable pins or locks securing the panel to the frame
- All "glass" used in exterior sliding doors and fixed glass panels should be made of laminated safety glass or polycarbonate sheeting. Plexiglas or single-strength glass will not qualify.
- Doors should open on the inside track, not the outside track

The following are factors to consider when selecting the type and size of windows:

1. Requirements for light, ventilation, and view
2. Material and desired finish—wood, metal, aluminum, steel, stainless steel
3. Window hardware—durability, function
4. Types of glazing: sheet, plate, or float
5. Effectiveness of weather stripping
6. Appearance, unit size, and proportion
7. Method of opening (hinge or slider), choice of line of hinges

8. Security lock fittings
9. Accessible louver windows
10. Ground floor—recommend lower windows, large fixed glazing, and high windows, small openings
11. Size and shape to prevent access
12. Size because of cost due to vandalism
13. Use of bars or grills on inside
14. Glass:
    a. Double glazing deterrent
    b. Types of glass:
        - Acrylic glass, also known as Plexiglas or polycarbonate
        - Tempered glass and laminated glass
        - Wired glass and bullet-resistant glass
        - Mirrors and transparent mirrors
        - Electrically conductive glass
        - Rough or patterned glass
    c. Vision requirements
    d. Thickness
    e. Secured fixing to frame
    f. Laminated barrier glass—uses
    g. Use of plastic against vandalism
    h. Fixed, obscure glazing for dwelling house garages
    i. Shutters, grilles, and louvers for sun control and visual barriers as well as security barriers

Window Ironmongery

- Security window locks built-in during manufacture
- Security window locks fitted after manufacture
- Transom window locks
- Locking casement stays
- Remote-controlled flexible locks

Double-Hung Wood

1. All locking devices to be secured with ¾-inch full-threader screws.
2. All window latches must have a key lock or a manual (nonspring-loaded or flip-type) window latch. When a nonkey-locked latch is used, a secondary securing device must be installed. Such secondary securing devices may consist of
    a. Each window drilled with holes at two intersecting points of inner and outer windows and appropriate-sized dowels inserted in the holes. Dowels should be cut to provide minimum grasp from inside the window.
    b. A metal sash security hardware device of an approved type may be installed in lieu of doweling.

    Note: Doweling is less costly and of a higher security value than more expensive hardware.
3. Follow balanced design principle. The glass falls first approach; that is, the walls are stronger than the anchors, the anchors are stronger than the frame, and the frame is stronger than the glazing.

Windows require protection when they:

- Are less than 18 feet from ground level
- Are less than 14 feet from trees
- Have openings larger than 96 sq. inches

Bullet-Resistant Materials, Bullet-Resistant Glazing for a Secure Workplace

Total Security Solutions offers a full line of bullet-resistant glass in acrylic, polycarbonate, and glass-clad polycarbonate. These products are available at UL protection levels 1–8, providing protection against guns ranging from a 9 mm to a 12 gauge. These bullet-resistant products are typically used in banks, credit unions, gas stations, and convenience stores, but are appropriate for any business with cash on hand that wants to provide their employees with a secure work environment.

In addition to providing bullet-resistant products to glaziers and mill shops, Total Security Solutions provides custom milling and installation of secure barrier systems. Typical

materials used in construction or sold directly include:

- Interior/exterior transaction windows
- Bulletproof doors
- Ballistic counters
- Package passers
- Bullet-resistant barriers and framing
- Bullet-resistant transparencies and fiberglass

Bullet-Resistant Fiberglass Wall Panels

These are used to provide bullet-resistant protection to the walls of corporate executive offices, boardrooms, conference rooms, lobbies, reception area counters, customer service counters, and safe rooms. This bullet-resistant fiberglass can be installed by the manufacturer or even by a general contractor. Once installed, this product will never be seen but will provide high-quality ballistic protection and peace of mind for years and years to come.

Bullet-Resistant Doors

Along with protection for the walls and lobbies of offices, there are a wide variety of bullet-resistant doors to meet different needs, for example, solid executive-style veneered doors to match existing doors but with bullet-resistant protection. Again, this is invisible bullet-resistant protection, therefore, nobody will know it's there. In addition, there are also full-vision clear doors, half-vision clear doors, plastic laminate no-vision doors, and bullet-resistant steel doors. All of these doors are prehung, so any contractor can install them within minutes.

Bullet-Resistant Windows

Bullet-resistant windows can be custom built for the needs of each individual client. Office windows can be replaced with bullet-resistant windows ranging from levels 1–5, or existing windows can be left in place and a second bullet-resistant window can be added behind the existing window in such a way that it will be virtually invisible to the general public.

Bullet-Resistant Executive Office Products

The following can be used for offices, boardrooms, and conference rooms:

- High-quality executive-style bullet-resistant doors
- Bullet-resistant wall armor to line all the walls of an office
- Bullet-resistant custom-made windows to protect all existing window locations
- High-security electronic mag-locks to lock doors in the event of an attack

Bullet-Resistant Transaction or Reception Area

- Bullet-resistant transaction window systems
- Package exchange units
- Bullet-resistant reception door with electric strike
- Bullet-resistant fiberglass for reception counter die wall
- Stainless steel deal trays for small transactions

Residential High-Level Security for Corporate Executives

- Provide bullet-resistant protection at point of entry (garage, front doors, front windows, etc.)
- Build safe room including walls, doors, windows, high-security locksets
- Convert closet into a high-level safe room
- Convert master bedroom into a high-level safe room (add invisible bullet-resistant protection to all walls, doors, and windows)

Finally, be advised that there are standards that apply to these installations and products.

WINDOW FILM

Window film isn't bulletproof and there is *no* film product out there that is. Window film can be resistant to small arms and shotguns, however. Lumar window film products have a bomb blast proof film product.

Window film comes in four categories:

1. **Security or safety film.** The benefits are an outer pane of glass may break but the inner will stay intact. It is used to protect retail, commercial, and residential buildings and other types of window structures from the damages of flying glass due to earthquakes, windstorms, attacks, vandalism, theft, and accidents.
2. **Decorative film.** This makes glass surfaces clear and visible, enhances safety in public spaces, and allows you to customize your space with a corporate logo.
3. **Anti-graffiti window film.** This is a protective film that helps prevent scribling or other defacing a base surface. The film is easy to peel off and replace, eliminating graffiti and the cost to replace glass.
4. **Solor film.** This has many benefits, such as it reflects and absorbs heat and light and it increases energy efficiency, reduces HVAC cost, protects furniture and carpets, and provides greater temperature stability.

REFERENCE

[1] Stegbor, Security data sheet, V1. Available at www.stegbor.com, 2011.

ADDITIONAL WEB RESOURCES

International Window Film Association, www.iwfa.com
Extreme Window Solutions, www.extremewindowsolutions.com
Ace Security Laminates, www.acelaminate.com
Total Security, www.securityfilm.biz/index.htm
Pacific Bullet Proof, www.pacificbulletproof.com

CHAPTER

20

Doors

Marianna Perry, MS, CPP, Lawrence J. Fennelly, CPO, CSS, HLS III

INTRODUCTION

No book on physical security would be complete without talking about doors. If you have ever been to a place like Home Depot you know doors come in all sizes and shapes—hung on the right, hung on the left, 1-inch dead bolts, a mortise lock, etc., or it's hollow core, solid core, wood, or metal. Without getting too technical we will discuss the many types of doors and hardware attached.

There are two types of flush doors: hollow core and solid core. A hollow-core door is literally nothing more than two sheets of a thin substance overlaying hollow cardboard strips. A solid-core door has a substantial security advantage over a hollow-core door. Continuous block cores, a common type of solid-core construction, are composed of wood blocks bonded together with end joints staggered and sanded to a smooth, uniform thickness.

Strictly from a security perspective, a metal, steel-sheathed door is superior to any type of wood door. A flush metal door comes with a metal frame, usually reinforced by interior formed sections. Metal doors are, however, less attractive and offer less insulation than wood doors.

A door system includes the door, frame, and anchorage to the building. As part of a balanced design approach, exterior doors in high-risk buildings should be designed to withstand the maximum dynamic pressure and duration of the load from an explosive blast. Other general door considerations are:

- Provide hollow steel doors or steel-clad doors with steel frames.
- Provide blast-resistant doors for high threats and high levels of protection.
- Limit normal entry/egress through one door, if possible.
- Keep exterior doors to a minimum while accommodating emergency egress. Doors are less attack-resistant than adjacent walls because of functional requirements, construction, and method of attachment.
- Ensure that exterior doors open outward from inhabited areas. In addition to facilitating egress, the doors can be seated into the doorframes so that they will not enter the buildings as hazardous debris in an explosion.
- Replace externally mounted locks and clasps with internally locking devices because the weakest part of the door system is the latching component.
- Install doors, where practical, so that they present a blank, flush surface to the outside to reduce their vulnerability to attack.
- Locate hinges on the interior or provide concealed hinges to reduce their vulnerability to tampering.
- Install emergency exit doors so that they facilitate only exiting movement; if these doors have portable alarms remember to change batteries and check on systems annually.

- Equip any outward-opening double door with protective hinges and key-operated mortise-type locks.
- Provide solid doors or walls as a backup for glass doors in foyers.
- Strengthen and harden the upright surfaces of door jambs.

RESIDENTIAL BUILDINGS

Exterior Doors

1. All exterior doors, except sliding glass doors or metal doors, with or without decorative moldings, should be either solid-core wood doors or stave, or solid wood flake doors, and should be a minimum of $1^3/_4$ inches in thickness. No hollow-core door or hollow-core door filled with a second composition material, other than just mentioned, is considered a solid-core door.
2. All exterior door hinges should be mounted with the hinge on the interior of the building, except where a nonremovable pin hinge or stud bolt is used (such hinges may be installed with the hinge facing the exterior of the building).
3. The shim space between the door buck and doorframe should have a solid wood filler 12 inches above and below the strike plate area to resist spreading by force applied to the doorframe. Screws securing the strike plate area should pass through the strike plate and doorframe and enter the solid wood filler; a minimum of 3- or 4-inch screws should be used to secure a doorframe. The screws should also enter the solid wood filler at least ¼ inch.
4. No glazing may be used on any exterior door or window within 40 inches of any lock, except
   a. That glass should be replaced with the same thickness of polycarbonate sheeting of an approved type. (Plexiglass should not be used to replace glass.)
   b. That door locks should be a double-cylinder keyed lock with a mortised dead bolt that extends into the strike plate a minimum of 1 inch.
   c. *French doors* should have a concealed header and threshold bolt in the stationary, or first/closed door, on the door edge facing.
   d. *Dutch doors* should have a concealed header-type securing device interlocking the upper and lower portions of the door in the door edge on the door strike side provided that a double-cylinder lock with a 1-inch dead bolt is provided on the upper and lower sections of the door and the header device is omitted. You should also check about ADA compliance on doors as well as with the Builders Manufactures Hardware Association (BHMA) for changes in door standards. In addition, you should check before double-cylinder dead bolts are installed in residential buildings that it is in compliance with local fire safety and life safety codes.
   e. *Sliding glass doors:*
      - Sliding glass doors should be installed so as to prevent the lifting and removal of either glass door from the frame from the exterior of the building. Consider secondary locking systems.
      - Fixed-panel glass doors (nonsliding) should be installed so that the securing hardware cannot be removed or circumvented from the exterior of the building.
      - Each sliding panel should have a secondary locking or securing device in addition to the original lock built into the panel. The second device should consist of a Charley bar–type device, a track lock, a wooden or metal dowel, or inside removable pins or locks securing the panel to the frame.
      - All "glass" used in exterior sliding glass doors and fixed glass panels is to be laminated safety glass or polycarbonate sheeting. Plexiglass or single-strength glass does not qualify for this program.

Exterior Doors in Commercial or Business Applications

- Should be numbered on the interior and exterior so they can be easily identified in the event of an emergency. Use clockwork numbering.
- Should have signage indicating whether the door is to be used for an emergency exit, employee entrance, authorized personnel only, or directing all visitors to enter through a specific door. People accessing the building need to be directed to the appropriate door.

Mechanical Locking Devices

Locks come in a variety of shapes and sizes, each having a specific purpose, for example, warded locks, lever locks, pin tumbler locks, multiple axes tumblers, wafer tumbler locks, interlocking pins, electromagnetic locks, electronic locks (crash bars), electromechanical locks (breakaway strikes), and combination locks.

Strike Plates

A strike plate comes with every door lock. Many times strike plates are cosmetic and not intended to provide much security. The strike plate's attachment to the doorframe is usually the weakest point in the entire door/doorframe/lock system.

High-security strike plates are available. They sometimes come with a heavy-gauge metal reinforcing plate that mounts under the cosmetic strike plate and come with 3-inch-long screws that secure the strike to the wall framing, not just to the doorframe jamb. The screw holes are staggered so the screws don't penetrate into the same grain of wood. The concept of screwing into different wood grains in the doorframe and wall framing is to make it more difficult to split the wood doorframe or wall framing when the door is impacted. *This feature should be considered at every exterior door and at doors coming from attached garages.*

THE FUNCTION OF A DOOR

The modern equivalent to the cave dwellers' animal skin is the door. The function of a door in physical security is to provide a barrier at a point of entry or exit. The function of a door in maximum security is still to provide such a barrier, however, the barrier must also be impenetrable by ordinary means and offer the maximum delay time before penetration by extraordinary means (i.e., by the use of cutting tools, hand-carried tools, and some explosives).

During construction of a maximum-security facility, it is necessary to define the function of all doors and their relationship to the total protection system. When an existing door is evaluated, the function must again be defined and include the area or material protected.

It is not necessary to make all doors maximum security—only those that are essential to the effective functioning of the total security system. Once a particular door is designated to be incorporated into the overall system, it must be upgraded to provide maximum security. There are two options in this respect: one can replace the door with a commercially available, penetration-resistant model, or upgrade it to provide the necessary resistance. Obvious areas of concern when dealing with maximum security doors are door hinges and hardware [1].

Case Analysis

The Chula Vista, California, police department undertook an extensive study of the factors that attracted burglars to specific homes, as well as those protective devices that were most effective at preventing burglaries. Researchers and sworn police staff interviewed more than 300 victims and suspects, conducted more than 100 street-view environmental assessments, and reviewed over 1,000 incident reports of burglaries committed against single-family homes. Key findings from the analysis phase included:

- Doors without deadbolt locks were targeted.
- Windows with single panes were targeted.

- Windows with simple stock latches were easily defeated.
- Sliding glass doors without specialized pin locks were easily rocked off their tracks.
- Almost all targeted properties had numerous hidden points of entry concealed by high shrubbery or solid fencing.

Chula Vista negotiated with the five major home developers in the city to make small, but significant, design changes to address the key risk factors and protective elements for residential burglary identified in the analysis phase. These changes were made in every new home built in the city after February 1999. Developers also agreed to distribute anti-burglary literature tailored to Chula Vista residents at the point of sale [2].

Terminology

Levers. Levers are used in some mortise locks and padlocks. The higher the number of levers a lock contains, the higher the level of security it offers.

Electric strike. An electrical device that permits releasing of the lock in the door from a remote control.

Dead bolt. On a mulipoint lock, the dead bolt is located at the center of the lock to add increased security. It is normally of rectangular shape, but can also be in the shape of a hook.

Flag hinge. A door hinge system used on PVCu doors that allows for easy installation and adjustment.

Mortise lock. The lock fits into a mortise that has been "cut out" of a timber door edge. The locking action is achieved by a bolt that shoots out of the lock into the striker plate when the key is turned.

Rim lock. Night latches are still sometimes referred to by their traditional name, "rim-locks," although a rim-lock usually now refers to a basic security lock for use on internal doors, gates, or outbuildings.

Thumb-turn cylinder. A knob fitted to one end of a cylinder that allows the door to be unlocked without a key from one side only.

Standards for Doors

Standards that apply to doors have been implemented or produced and supported by the Architectural Manufacturers Association (AAMA); ANSI; American Society for Testing and Materials (ASTM); National Association of Architectural Metal Manufacturers (NAAMM); NFPA 80, 2007, and NFPA 101, 2009; the Steel Door Institute (SDI); Underwriters Laboratory 305 (UL); and the International Standards Organization (ISO).

REFERENCES

[1] Fennelly, LJ, ed. Handbook of loss prevention and crime prevention, 5th ed. 2011, Waltham, MA, Ch. 9.
[2] The Chula Vista, CA, Residential Burglary Reduction Project, 2001 Chula Vista Police Department.

CHAPTER

21

Physical Security*

Dr. Gerald L . Kovacich, Edward P. Halibozek

"Paradise is now shut and locked, barred by angels, so now we must go forward, around the world and see if somehow, somewhere, there is a back way in."

—Heinrich von Kleist

This chapter introduces the fundamental principles of physical security. The concept of security in physical layers is introduced and external barriers (e.g., fences, walls, gates, buildings, and lobbies) and internal barriers (e.g., access control systems) are addressed. Internal controls and intrusion detection systems are also addressed, as is the use of current technology such as biometrics.

DEFINITION OF PHYSICAL SECURITY

No business is without security problems and assets protection risks. These risks and problems take many forms. Effectively mitigating them is not a happenstance occurrence. Problem elimination and risk mitigation require planning and an understanding of security needs, conditions, threats, and vulnerabilities. Assessing security conditions and planning for appropriate levels of assets protection begins with the basics: risk management.

Physical security is the most fundamental aspect of protection. It is the use of physical controls to protect the premises, site, facility, building, or other physical assets. The application of physical security is the process of using layers of physical protective measures to prevent unauthorized access, harm, or destruction of property. In essence, physical security protects a property, plant, facility, building, office, and any or all of their contents from loss or harm.

Physical security contributes to the protection of people and information. Sophisticated protection measures, other than physical, are employed to protect people and information. Nevertheless, physical security measures are part of the overall protective package. They are the baseline security measure, or foundation, on which all other security measures and functions are built.

Physical security measures are used to ensure that only authorized persons have access to a facility and property. The measures employed must be appropriate for each separate operating environment. A manufacturing facility requires physical security measures and functions and controls that may differ from those used at one of the sales offices. Manufacturing facilities in different parts of a country or in different countries generally require differing physical security

*Kovacich, GL, and Halibozek, EP. The manager's handbook for corporate security. Boston: Butterworth-Heinemann, 2003, pp. 186–206. Updated by the editor, Elsevier, 2011.

measures—one size does not fit all. In any event, physical security measures are the baseline of protection. All other security measures will be integrated with physical security measures, developing a protection profile of assets protection within layers.

It is the responsibility of the corporate security manager (CSM) or higher to determine what physical security controls are necessary to provide an adequate level of protection. To do this, the CSM must know the facility or site layout. The CSM must understand the operating requirements and operation of the enterprise, conduct an initial physical security survey, and periodically conduct supplemental surveys as part of the CSM's risk management survey program. This will allow for a thorough understanding of threats and vulnerabilities and enable the development and implementation of sufficient controls.

SECURITY IN LAYERS

What physical security measures are used to protect assets depends greatly on what assets need to be protected, where they are located, and what threats, vulnerabilities, and risks pertain to them. Applying an appropriate level of protection for each environment requires a specific understanding of that environment. To best accomplish this, you should start at the beginning.

Physical security measures should be designed into a facility during the facility design phase and built into the facility during the construction phase.

Ideally, architects and security professionals would work together taking into consideration all aspects of assets protection requirements applicable to the proposed operating environment. This type of planning helps create optimum security at the lowest possible cost. If done properly, security problems created by so many buildings being designed without any consideration given to security controls would no longer be the issue that they usually are these days.

As the CSM, if you are not working with new construction and are occupying an existing building, designing in architectural security may not be possible. If retrofitting or renovation of the site or facility is necessary to accommodate the new business operating environment, then security may still be considered as part of the design. If not, physical security issues should at least be addressed prior to occupancy or operation. Security problems resulting from a failure to make security part of the design and construction phase will probably be of a structural nature and too expensive to undo or fix. The only solution in this case is the application of protective measures that otherwise might not have been needed, thus adding costs. Since the CSM knows that the foreign facilities will be moved, it is important that the CSM coordinate the move to facilities that meet the assets protection physical security criteria, or arrange to locate to another facility, or modify the existing facility before the move takes place.

The application of physical security controls should be approached in layers. There is no single physical control that will fulfill all security needs. Layering controls from the outer boundaries of each of the facilities to the inner boundaries will allow you to build a security profile to meet specific security needs.

OUTER LAYERS OF PROTECTION

The outer layers of protection for a facility depend on the type of facility and its location (Figure 21-1). For example, an office building located within a city may only have as its outer layer, or perimeter, the walls of the building, whereas a manufacturing facility located in an industrial district may be on a large parcel of land with parking lots, storage areas, and grounds surrounding the building or buildings. On a facility of the second type, the perimeter is usually a barrier, such as a wall or fence, located at or near the edge of the property line.

The perimeter of a facility takes many forms. For an office building it may be the building walls. For a factory it may be a fence line or a wall at the property edge. The outermost layer of protection could also be a highway; a natural physical barrier, such as a river, lake, or other body of water; or other human-made barriers. Whatever

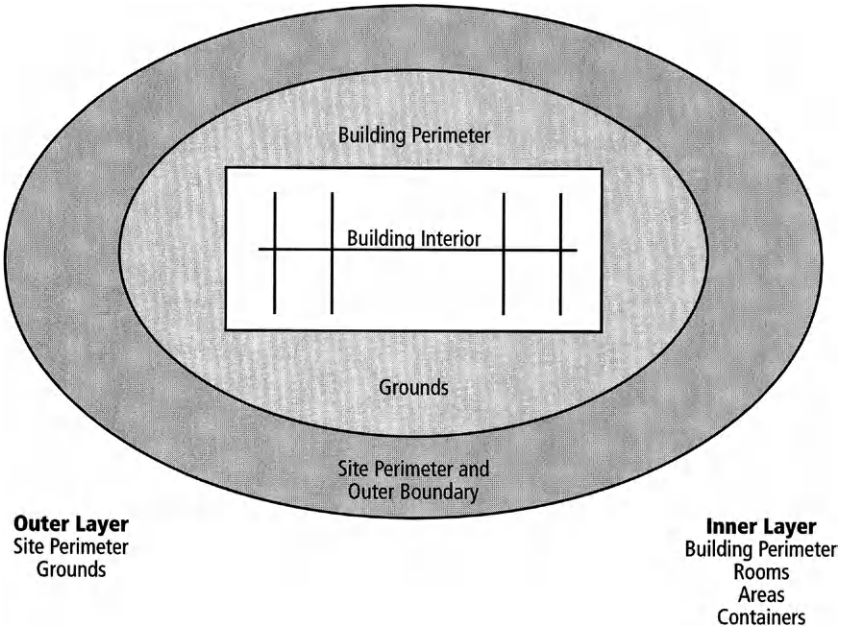


FIGURE 21-1 Illustration of layers within a site, facility, and building.

the barrier, it is the first layer of physical security. It may be at the perimeter's edge or inside the perimeter. Regardless of where it is situated, it is the layer of first control. Inside the outer layer, the use of other layers of physical security may be necessary.

Grounds

Not all facilities have grounds. Grounds serve many purposes. They may be purely decorative to create a pleasant environment for customers and employees. They may be functional and serve as a place to locate storage areas and warehousing facilities. They may also serve as a buffer or barrier between the perimeter of the facility and the buildings where work is done and people, physical assets, and information are housed. If kept clear, grounds serve as a clear zone, allowing for unobstructed observation of the area. If used for storage or other purposes, they should be kept organized and maintained. In this way, disruptions are easier to identify and the risk of hazards is reduced.

Roads

Roads are both necessary and problematic. They allow employees and customers to have easy access to the facility. However, they also allow unauthorized personnel to have easy access to the facility. The degree of control necessary on all roads leading to your facility will vary. Any controls used will depend on the type of road and its use. Is it a public road or a private road? Public roads do not allow for additional controls. They belong to the municipality, city, or state, and exist to facilitate movement of vehicles and people. If a facility is adjacent to a public road, controls can begin only where the road ends and your property begins. Private roads allow for much greater control. Owners of private roads can install controls that allow for restricted passage. Owners of private roads can make the determination as to who has access and under what conditions. Ideally, controls on any road should begin as close to the outer perimeter as possible.

In an office building environment, public roads generally lead to parking lots that are often adjacent to the buildings. This means perimeter controls begin at the parking area or at the walls of the buildings.

Fences, Walls, Gates, and Other Barriers

There are two types of barriers used for perimeter protection: natural barriers and structural barriers.

- Examples of natural barriers include rivers, lakes, and other bodies of water; cliffs and other types of terrain that are difficult to traverse; and areas dense with certain types of plant life (e.g., blackberry bushes that are very thorny and dense).
- Examples of structural barriers include highways, fences, walls, gates, and other types of construction that prohibit or inhibit access.

None of these barriers completely prevent access. They do, however, make it more difficult for unauthorized persons to gain access. When used with other layers of physical control, they can be very effective.

Fences. The most commonly used form of barrier, other than the walls of a building, is a fence. Fences vary in type, size, use, and effectiveness. They are erected quickly for a reasonably low cost, as is the case with the basic chain-link fence. They are made more complicated and effective by adding barbed wire or concertina wire, alarm systems, or double fencing with alarmed clear zones between. The type of fence selected and used is determined by the specific needs. Again, balance the costs versus the risks.

If a factory perimeter does not have the advantage of a natural barrier, fencing is necessary. The fencing used can be very typical. For instance, it is 7 feet high and made with 9-gauge wire. It rests no more than 2 inches above the ground and in areas where the soil is loose. A concrete trough/border lies at the base to prevent gaps from erosion or human intrusion. At the top of the fence is a "guard" of three strands of barbed wire placed at a 45-degree overhang that faces away from the property. This actually extends the height of the fence by 1 foot and provides added difficulty for anyone attempting to scale the fence. Naturally, buildings, structures, and trees are sufficiently far away from the fence line as to not offer assistance to those who would attempt unauthorized entry. When looking at enhancing physical security at one of the factory properties, the physical security project leader advised the CSM to consider a "good neighbor" policy. This policy states that the local city planning and beautification commission must also approve any changes made that affect the beauty of the surrounding area.

Walls. Walls serve the same purpose as fences. They are human-made barriers but generally are more expensive to install than fences. Common types of walls are block, masonry, brick, and stone. Walls tend to have a greater aesthetic value, appealing to those who prefer a more gentle and subtle look. Regardless of the type of wall used, its purpose as a barrier is the same as a fence's. To be most effective, walls ought to be 7 feet high with three strands of barbed wire on top. This will help prevent scaling. For aesthetic reasons, management may resist the use of barbed wire. Nevertheless, it should be seriously considered.

Walls also present a disadvantage in that they obstruct the view of an area. Chain-link and wire fences allow for visual access on both sides; walls do not. This obstacle is overcome by keeping clear zones for several feet on each side of the wall and by using video cameras for observation. Use of roving patrols also increases visibility. When the walls of a building serve as a perimeter barrier in lieu of fencing, the issues are different. Scaling the wall to get to the other side is not an issue, but access to the roof is. Furthermore, controlling access to other openings in the building becomes more critical when the walls to the building are the only outer barrier separating the outside world from the assets requiring protection.

Gates. Gates exist to both facilitate and control access. The most secure perimeter allows no one through. However, that is not practical or

desirable; people must come and go. Employees, customers, and other visitors need to have easy access to a facility. Gates allow for this.

Gates need to be controlled to ensure that only authorized persons and vehicles pass through. A variety of controls are used, for example, guards; electronic interactive access control systems, such as card key or password access; or remote control access with video camera observation. What you select depends on your specific needs and conditions (e.g., acceptable risk levels). The number of gates to a facility should be kept to the minimum necessary, not the minimum desired. Controlling gates requires using resources. The more gates used the more resources it will take and the more potential problems are created, because any opening is always a potential vulnerability.

Gates when not in use should be locked or eliminated. Having the flexibility to open an additional gate when traffic demands are high is useful. Eliminating a potential vulnerability is more useful. If a periodic need for an additional gate does exist, when the gate is not in use it must be closed, locked, and monitored. Monitoring is done by video camera by roving patrols, or through the use of an alarm system.

Periodically, even monitored gates require physical inspection to ensure they are operable and secure.

Natural Barriers. The effectiveness of a natural barrier will depend on the barrier itself and how it is used. A body of water may be very effective in keeping pedestrian traffic away from your property but not very effective at keeping boat traffic from your property. In this case, a natural barrier needs to be augmented with a human-made barrier. In any case, natural barriers, like human-made barriers, need to be monitored. Cliff sides can be scaled, water can be crossed, and difficult terrain can be overcome.

Other Openings. Openings not designed for personnel or vehicle traffic are also a concern and must be secured. Needing control are sewage pipes, drains, utility tunnels, large conduits, and heating, ventilation, and air conditioning ducts. Where it is appropriate to lock them, they should be locked. Those that cannot be locked should be monitored. Monitoring is in the form of an alarm system or physical inspection. Any opening larger than 96 square inches should have doors, bars, or grillwork in place to prevent human access. These are installed as permanent or removable, with locking devices. For example, to prevent access through heating, ventilating, and air conditioning ducts, man bars can be installed inside the ducting. This is not practical for openings requiring access by maintenance personnel, where the use of removable grills or doors may be more practical. In any configuration, all openings must be assessed for vulnerabilities and appropriate protective measures implemented. Regular inspections or monitoring to ensure tampering has not occurred is essential.

Buildings and Doors

For many facilities, buildings and doors define where the outer layers of security end and the inner layers of security begin. Within a site, buildings are the separation point between the outer and inner layers of security controls. In the area between buildings and the outer perimeter (usually a fence line) of the facility lie a variety of security controls that make up the entire outer layer of security. In this configuration, it is best to keep the areas adjacent to building and door exteriors clear. In essence, create a clear zone of 10–15 feet where no storage, parking, or regular activity is authorized. Maintaining a clear zone allows for unobstructed observation by surveillance cameras and guards. Visual access to the clear zone becomes the first line of defense for the inner perimeter.

Parking

Providing parking space for employees, customers, and visitors is necessary. Unless the business is small and located on a street with public parking access, parking needs to be provided. Parking should not be allowed within the outer perimeter. Vehicles inside the perimeter make it easier for theft to occur. Employees with immediate access to vehicles inside the perimeter have a ready place

to conceal stolen items. Furthermore, unless all vehicles are inspected, it will not be known what items of contraband or weapons are brought into the facility. If, for lack of space, parking must be permitted within the outer perimeter, additional fencing should be erected to separate the parking area from the remainder of the facility.

Parking can be a very sensitive subject. Where people park is often linked with their status within the company. City and state laws require sufficient parking to be set aside for disabled persons. Visitors like to park close to the areas they visit. Parking is difficult to manage and police. It is recommended that parking rules be established by senior management or the human resources department with the CSM's input. Parking enforcement should be handled by security.

Company-owned vehicles are the only exception to parking within the perimeter. Protection is particularly important if the vehicles are loaded with merchandise, supplies, or raw materials. They should be parked in a secure, well-lighted area, and locked. However, they should not be parked in the same area as privately owned vehicles.

Lighting

Lighting serves several purposes. Adequate lighting reduces the possibility of accidents and injury. It also serves as a deterrent to would-be intruders. With adequate lighting, the grounds, fences, walls, and buildings can be clearly observed. Guidance for specific levels of illumination is obtained through federal sources or from any company that sells or installs exterior and parking lot lighting. The best determination for assessing adequate lighting is conducting an actual test. Is the existing lighting sufficient as assessed under controlled and practical conditions? If not, you need more lighting.

Adequate lighting serves as a deterrent. Intruders are less likely to enter well-illuminated areas, fearing they will be observed. Lighting should be sufficiently protected to prevent tampering and destruction. It should be kept within the perimeter to reduce the possibility of damage. Lights should be placed high enough to ensure that tampering must be deliberate and difficult. When used as a deterrent, lighting should have a backup power supply in the event of a power disruption. Lighting requires little attention in that it can be programmed to turn on and off at specific times. It can be light-, movement-, or heat-sensitive. It can be linked to alarm systems and support CCTV. After installation, it does require frequent inspection to ensure all systems are operational.

Specific lighting needs vary with each site or facility. As part of a site physical security survey, lighting should be considered. Areas that require direct protection should have lighting that not only illuminates the area but also does not interfere with security's ability to effectively monitor. Too much lighting can create a problem by producing bright spots that blind people and cameras. Doors, gates, and other entrances should be well illuminated. This allows for safe passage and for better observation by guards and cameras. Areas with heavy personnel and vehicle traffic also require good lighting, as it reduces hazards and increases visibility. Large open areas with little traffic can use less lighting, but lighting must be sufficient to allow for general security observation and a safe environment.

This is sometimes a political issue in that executive management wants to lower utility costs, among other costs. Management sees security lights on in the daytime and complains to the CSM. All of a sudden the CSM has a directed task to see how much utility (e.g., electricity) costs are due to security. Management also wants to know how the costs can be reduced. If the CSM had thought about such a possibility early on, the return on investment for solar-powered lighting could have been considered. If solar-powered lights were installed they could be left on indefinitely with no electrical power costs involved. Of course, some executive managers still might not be satisfied. They might say, "Yes, but it gives a bad impression to those who don't know they are solar powered," or, "Ah yes, but we can save money on the lightbulbs because they will burn out quicker if left on continuously." Sometimes a CSM can't win.

Surveillance

Surveillance is an important tool for security in its effort to protect assets. Generally, surveillance is accomplished by using security guards or surveillance cameras. Frequently, a combination of both is used to achieve maximum observation and effectiveness for any facility. As part of a site physical security survey, the need for surveillance should be identified. This need should be assessed against the existing practice and capability. With this information, a plan for site or facility surveillance can be developed. The plan considerations are:

- Purpose of surveillance—deterrence or observation
- Identify critical or high-risk areas
- Camera and guard mix
- Location of cameras
- Recording capability needed
- Need for hidden cameras
- Type of cameras needed—wide or narrow angle of view, low or high level of light, availability of solar-powered cameras

Each choice has its strengths and limitations (Table 21-1).

The CSM, lacking in some resources, looks for alternative ways of providing assets protection in areas where there was no budget available for cameras. The CSM discusses the matter with the supplier of surveillance cameras. The CSM is able to obtain free outdated and broken cameras. These are installed, with the LED powered by several batteries, indicating that the camera power is on and working. Appropriate signs advising of the surveillance cameras are posted in the area. To those passing through the area, it appears as if active surveillance cameras are installed and used. Such techniques have the same effect as active cameras; however, be advised that this is not a cure-all for expensive surveillance cameras. The cameras do not see miscreants' activities in that area, and therefore there is no patrol guard response. However, it is something to consider when the surveillance camera budget is limited.

Alarms

Alarms are one of the layers used in the many layers of protection for a facility. How they are used and to what extent should be determined in the planning process. The site physical security survey should identify vulnerabilities, current and potential, and the layers of protection in use. When assessed against known or suspected threats, the need for alarms to augment physical protections should be apparent.

Alarms augment barriers and guards. They call attention to problems not stopped or prevented by barriers and not observed by guards. In essence, they enhance the detection process.

TABLE 21-1 Strengths and Weaknesses of CCTV and Guards When Used in the Surveillance Process

	Strengths	Weaknesses
CCTV Camera with recording capability	Serves as a deterrent Flexibility of recording Permanent record Reduced insurance rates Deterrent for crime Multiple angles of view Night view, works in low light	Cannot respond to incident Cost of initial installation Maintenance cost Employee perception of being watched
Guards or security professionals	Can act on observation Deterrent Mobility Apply immediate judgment	Cannot watch everything Human error No permanent record of observation Limited angles of observation

However, they also serve as a deterrent. Since most physical security controls include the use of alarm systems, intruders can assume they are part of the protection profile.

Alarm systems are used to call attention to an immediate problem. Unlike physical barriers (e.g., walls, fences, or gates), they are not a physical obstacle in and of themselves that are used to slow down or stop an intruder. They are an alert mechanism used to call attention to an intruder or problem. Audible alarm systems may serve as an obstacle much more than silent alarm systems, since they let everyone in the general area know when there is an alarm activation.

There are many types of alarm systems. Within the physical security profile, intrusion detection and fire detection are used the most. As part of the outer barrier, intrusion detection is used to indicate penetrations in or between the various layers of protection. Different types of alarm systems are available for fences, gates, and walls, and all provide an alert if they are compromised.

Alarm systems are used as part of the protection profile for both inner and outer layers of physical security. When used as part of the outer layer of protection, they serve as an advanced warning notice that an outer layer has been compromised, thereby making the inner layers more vulnerable. They serve to protect property and assets stored within the outer layer by providing an indicator that an intruder is tampering with, or in the area of, the property being protected.

In any case, alarms are only effective if there is a response. Someone must react to an alarm. An alarm system without timely response is not effective. Responding to an alarm is essential, or the alarm becomes nothing more than an expensive annoyance (e.g., car alarms in public areas are generally ignored). Perpetrators often test alarm systems by causing their activation and watching for a response. No response lets perpetrators know that they have plenty of time to work with. Responses to alarms by security guards or others must be periodically tested and the response of the security guards or others timed. These must be no-notice tests—it is ridiculous to test security guard responses if they know a test is to be conducted.

Alarm systems provide balance for the overall physical security profile in both protection capabilities and costs. Alarms can reduce the need for a large, stationary guard force. They allow for a configuration of alarm monitors, respondents, and some form of patrol. They reduce or even eliminate the need for a stationary force. If alarm systems are not used, the function they serve must be fulfilled by using a larger guard force, or through the use of greater surveillance capability, or you can just assume a greater risk level. Remember that it is not up to you to assume a greater risk level by choosing not to install alarms in an effort to save money. Actually, alarms save money by replacing people in many instances. Before assuming additional risk caused by the lack of alarms, you must consult with executive management and have them accept that additional risk level.

Alarm systems cost more to install than to maintain. The cost of alarm systems is greatest in the acquisition and installation phase. Once installed, maintenance and monitoring costs are generally much less than personnel costs. A return on investment can be calculated and used as a selling point on the value of alarm systems. Using alarm systems offsets the need for some guards. The savings in recurring guard costs can be compared to the cost for acquisition and installation of alarm systems. Over several years, it is usually more cost effective to use alarm systems to augment security than to rely on a larger guard force.

Do you want a silent alarm that is only audible in the manned security command center, or an alarm audible in the area that is alarmed and also at the security guard's console? The correct answer is, "It all depends." It depends on the area alarmed, the value of the assets located therein, the risks to those assets, and so forth. The key is to base your choice on a risk assessment or physical security survey of each particular environment.

INNER LAYERS

In the previous section we discussed elements that are generally considered to be part of the outer perimeter. They are the outer layers of

physical security. For the most part they are layers of physical protection that lead up to the building walls. We also indicated that, depending on the environment of the outer perimeter, you as the CSM might actually begin security at the building walls. In this situation, the first layer of security is made up of the walls, doors, and windows of a building. Office buildings in urban environments represent a good example of this situation. Outside these buildings are conditions that are not controlled by the building occupants. There is a single layer of outer physical security controls protecting the inner layers, which doesn't leave much room for error. In this case, penetration of a single layer allows access to the inner layers. This condition should lead to a greater emphasis on the types of inner controls applied.

Buildings, Doors, Windows, and Glass

Buildings serve as perimeters. In urban areas, the walls, doors, and windows of office buildings may be the outermost perimeter and the only outer layer of security control for the entire facility. In other settings, buildings may serve as part of the outer perimeter or as the first layer of the inner perimeter. This will depend on the individual facility configuration. Whatever layer of protection it provides, full consideration must be given to all aspects of building protection. All openings must be addressed, and buildings generally have many of them. Doors, windows, and passageways for ducting and conduits all need to be controlled. Power, communications, and heating, ventilating, and air conditioning systems require entry points from the exterior of the building into the interior of the building. To ensure they are not used for unauthorized purposes, controls should be in place. Any openings that serve no useful function should be permanently closed.

Functional openings larger than 96 square inches should be modified to prevent human access. Windows should be locked and alarmed. Alarms should detect entry or tampering. In some cases, man bars or screening are necessary. Screens and man bars allow for the passage of air and visual inspection but do not allow for human access.

The type of glass used in windows will vary depending on the location or use of the window. Windows at ground level on a perimeter wall clearly require a stronger glass than those windows located on higher floors or inside the outer perimeter. In some areas they may need to be bulletproof. Furthermore, special glass may be required, for example, in earthquake areas. Should such glass be shatterproof or shatter inwardly or outwardly? The answer is that it all depends. Using a risk assessment approach that includes personnel safety factors (e.g., flying glass) will assist the CSM in making a cost-effective decision. See Chapter 19 for more information on windows and glass.

Doors should be locked when not in use and controlled when in use. Controls range from guards at the door controlling entry and exit to mechanical or electronic access control systems requiring cards and card readers or access codes. Exterior or perimeter doors must be hardened, and are generally built to be stronger than interior doors. It may be necessary to have interior doors of a similar strength and quality as exterior doors if those interior doors are part of an area used to provide specific protection to high-value assets. All associated materials for doors must be consistent with the strength of the doors themselves. For example, a high-security door is of little use if weak latching devices or cheap locks are used to hold it in place. High-security doors should have high-security locks. Also look at the hinges. Are the hinges facing in or out; are they welded or is the pin removable? A locked door with hinges facing the direction of the potential penetrator does little good if the pins or hinges can be removed. See Chapter 20 for more information on doors.

Locks, Keys, and Combinations

Locks are an essential part of physical security protection. They are a cost-effective and simple

means of denying access to unauthorized persons. The largest expenses for locks are the initial purchase, installation, and control of their use. Depending on usage, little maintenance is required. Although any lock can be overcome, the higher the quality of the lock, the longer it will take someone to break it. Simple locks can be picked or easily damaged. More sophisticated locks will buy more time against any attempt to bypass them. Locks vary in quality and type and a wide variety are available. Determining the appropriate lock for any door, window, or other opening is based on planned usage, specific needs, and the assets requiring protection.

Perhaps the most vulnerable aspect of locks is the failure to properly protect locks, keys, and combinations; control is critical. Poor key control can render any locking device useless. Issuance of master keys must be severely limited, particularly the issuance of grand master keys. All locks, keys, and combinations should be accounted for. Keys and combinations should be issued in accordance with employees' need to perform their job. If there is no specific need, locks, keys, and combinations should not be issued. A permanent record of personnel issued or assigned keys or lock combinations must be kept. When keys are lost or stolen, the locks should be rekeyed. When a master key is lost, all affected locks should be rekeyed. There may be times when this is not necessary, such as if a key were inadvertently destroyed and its recovery or use poses no risk.

Keys should never be issued on a permanent basis. An annual assessment of locks, keys, and combinations needs and requirements should be made. This assessment will also assist in identifying lost or stolen keys or combinations that were not reported to security.

Locks, keys, and combinations should be issued to individuals rather than groups if individual accountability is a requirement. Sharing is a risk in that a theft or misappropriation of an asset protected by the lock cannot then easily be attributed to a specific individual. It is no different from sharing computer passwords.

Roofs

It is important to remember that roofs may be part of the outer or inner perimeter. Roofs generally have openings for maintenance, power, heating, ventilation, air conditioning, and other conduits. The same principles applicable to barriers and walls are applicable to roofs. Openings must be controlled. Since routine access to roofs is generally not an issue, locking devices and barriers such as screens and bars are used. Ladders or stairs leading to roofs should be controlled. Access to the roof should be made difficult for unauthorized personnel, but all fire regulations should be kept in mind.

Areas, Rooms, Containers, and Safes

Inside buildings there are open work areas, individual offices and rooms, storage containers, and safes. How they are protected depends on how they are used and on the value of the assets in them. Open work areas such as large cube areas, where many employees sit at workstations performing their daily duties, may not require additional controls. Once inside the building, employees and visitors may need to move freely in these areas. Since access authorization is verified at either the outermost layer of security control (outer perimeter gate leading into the facility) or the first control of the inner perimeter (door or lobby allowing entry into the building), additional checks for general access are not necessary—again, this is based on risk management. Moreover, access to general office areas and conference rooms, cafeterias, or rooms housing other employee services may not need additional controls. Employees in these areas must understand that they also have a responsibility for controlling access in that all individuals not known to them, or not wearing a current corporate badge, should be challenged as to their need to be in the area.

Areas or rooms where more sensitive work is done or sensitive information and materials are located require additional controls. The simplest means for applying these controls is through the

use of locking devices or access control systems on each entryway. From simple locking devices on doors to the use of electronic card readers or electronic personal recognition systems, varying degrees of physical controls can, and should, be used to limit access to sensitive work areas. The methods used depend on the application of a cost-risk philosophy.

Safes can be used for the most sensitive information or material. Safes are available in various sizes and strengths. Depending on the sensitivity of the information or material protected, simple combination lock or key lock safes may be sufficient. These safes can be obtained from a variety of manufacturers. For the most sensitive information and material, high-security safes and vaults may be necessary. For example, working with government classified material requires the use of government-approved storage containers. The higher the classification of government material, the more stringent the requirement for storage containers becomes.

ACCESS CONTROLS

Controlling access is a critical component of security in layers to protect corporate assets. Ensuring that only authorized personnel and vehicles enter and exit facilities reduces the risk of loss or damage to all assets. Effective access controls require the integration of different security functions that serve as individual layers of protection. Used as part of an integrated system, the following are useful access control tools:

- Security officers
- Locks—combination, code, or key
- Card reader systems—magnetic stripe, optical bar code, proximity cards, biometric systems (fingerprints, signatures, face or hand geometry, voice recognition, and retina recognition)

Part of the site physical security survey should focus on identifying access control vulnerabilities and existing access control practices. When vulnerabilities and existing practices are compared with what is actually needed, an access control profile that best fits your site can be developed and implemented. The access control profile must address who should have authorized access to the facility and under what conditions (e.g., weekdays but not weekends, normal business hours but not after business hours). It should also identify the individual security processes and tools needed to effectively design and implement proper access controls.

What Should Be Controlled?

Vehicles. All vehicles entering and exiting the facility must be controlled. Only authorized vehicles should be allowed on site. Procedures establishing traffic flow and parking need to be written and communicated. Violations of these procedures must be enforced. Not enforcing traffic and parking rules and regulations will quickly lead to a breakdown and abuse of controls. At the very least, consideration should be given to random inbound and outbound searches of vehicles to ensure that anything entering or leaving the facility has proper authorization.

Employees. Employees need easy access to their work areas, and access control procedures should be designed to facilitate their prompt and efficient movement in and out of the facility. Access control procedures should be the same for all employees, thereby creating a culture of respect and adherence to the process and practice. Requiring employees to use some form of identification to have authorized access to a site is a standard practice. Badges, access identification cards, and other forms of physical controls can be used to validate that a person is actually an employee and quickly allows him or her entry into or exit from a facility. If the site employee population is large (e.g., exceeds 50 people), do not rely only on personal recognition for access authorization. Personnel changes take place regularly, and keeping up with employee changes and turnover is better accomplished with automated systems than with the memories of security personnel. Furthermore, all employees should be subject to random entry and exit searches as determined necessary by the degree of assets protection required. To this practice there should be no exceptions.

Vendors, Suppliers, Customers, and Visitors. Very few people who are not employees should be allowed free and complete access to the facilities. If vendors or suppliers are assigned to a site on a full-time basis and do require unrestricted site access to perform their work, they are to be provided with identification that indicates that they are not employees. Moreover, this status should be subjected to scheduled periodic review to revalidate the need. Any identification provided to allow access should have an established expiration date. As with employees, all must be subject to random entry and exit searches. For contract employees, the expiration date of the badge should not exceed their contract expiration date.

How Do You Control Them?

Vehicle and Personnel Gates. The first line of protection for access to a facility is at the vehicle and pedestrian gates. Through these gates employees and visitors enter the facility, so control must begin there. Processes should be in place to allow employees through and to properly process all visitors according to established procedures or parameters. The use of employee identification badges coupled with an electronic card identification system is one of the most common tools used for this purpose.

Building Lobbies and Doors. The same controls used for gates are generally effective for lobbies and doors. Some lobbies have guards who are also receptionists, or receptionists who double as guards. In either case, it is important that these people understand that their priority is access control and being a guard rather than a receptionist. If there is a conflict in that dual role, the CSM should ensure the separation of those functions by having two individuals perform the separate functions (e.g., a receptionist as part of the human resources budget and a guard as part of the CSM budget). Executive management's idea is to have the lobby personnel appear very friendly and helpful. However, in some lobbies or access control areas they may want to provide the appearance of a no-nonsense security presence.

Interior Areas and Rooms. Inside a building, access is generally controlled by three effective mechanisms, two of which were discussed earlier:

- Lock and key devices
- Card key access systems and badges
- Other employees

Employees play an important role in controlling access to internal areas and rooms. When they encounter an unauthorized person inside an area or room, they should be trained to challenge that person and report the incident to security. This conditioning does not occur naturally, and will require employee awareness training to be conducted for all employees. Moreover, this type of behavior is best encouraged through positive recognition and reward.

Badges. The primary use of badges is employee identification. Badges can also be coupled with access control systems, expanding their use and effectiveness. Magnetic codes, bar codes, and proximity cards, which activate electronic locking devices, can be linked to the identification badge, making it a multifunctional identification and access tool. This tool can contain information pertaining to the specific characteristics of an employee. Identifying each individual by name and other specific personal information, such as photographs, encoded access authorizations, and pin numbers, is easily accomplished and makes the badge a very reliable authentication device. Sophisticated badge and access control systems are available from a variety of manufacturers. Computer technology and technology advancements in general have made the process of making badges more efficient, effective, and reliable.

To ensure reliability and effectiveness, the process of using a badge for employee identification must be controlled. Specific parameters for use must be established and maintained for the badge process to maintain its integrity. Rules governing the following aspects of a badge process will help ensure a very reliable system:

- Determine who is authorized to have a badge.
- Identify what data is needed on each badge.

- Security controls production, issuance, and accountability of badges.
- Badges must be recovered from employees who leave the company.
- Lost or stolen badges are reported and removed from the system.
- Worn or damaged badges are exchanged for new badges.
- A tracking system is used to ensure internal accountability of unused badge stock.
- A periodic review of the badge issuing process is conducted.
- Badges made but not in use must be controlled or destroyed.
- Tamper-resistant features such as holography should be used to make counterfeiting more difficult.
- Employees must understand the need for the badge process and adhere to proper usage.

At small facilities or small satellite offices, personal recognition is usually the best form of identification—as long as a process is in place to also identify those who have left the corporation. For larger facilities, generally with 50 or more employees, personal recognition is no longer practical and use of a more reliable employee identification system is needed. Badge systems generally fulfill this need. Again, the CSM must consider the risks of each option.

It is also necessary to control the access and movement of visitors, suppliers, and customers. For this, a badge process for nonemployees is used. It is similar to that of the employee badge process but more restrictive in the sense that it clearly identifies the visitor as someone who is not an employee and has obvious indicators on the badge calling out appropriate restrictions. Escort requirements, badge expiration dates, and specific areas authorized to visit are some of the useful data necessary for the visitor badge.

Employees must be familiar with the badge process. They should receive guidance and training as to how the process for employees and nonemployees works. Employees should be able to recognize authorized badges and react to unauthorized badges. Persons not wearing an appropriate badge or violating the parameters of the badge process should be challenged. Without the active participation of all employees, any badge process will be rendered ineffective.

Guards. Guards or plant protection officers are an integral part of a physical security profile. Depending on specific needs and the type of facility, their use will vary.

Guards add a human element to the physical security profile. They are used in situations where observation, training, and judgment are required to apply effective asset protection controls. For example, guards are often used for vehicle access control functions. They not only check proper identification of the vehicle and driver, but they also provide greater flexibility for vehicle inspection on a variety of cars and trucks that may have a need to enter the site. When an irregularity is observed, they possess the ability to react instantly to the situation by reporting or challenging those with questionable identification. Moreover, they make an assessment of a situation and determine if additional assistance is needed (e.g., responding to an alarm and determining whether an intrusion occurred or if the alarm was false).

Guards also provide the capability of patrolling a site or facility, making observations and taking note of changes or irregularities, all of which can be further investigated. The mobility of guards makes them particularly valuable, because their services are quickly applied to a particular need or situation.

One of the most common security functions outsourced is the guard force, since it obviously is human-intensive and one of the more costly aspects of an assets protection program. Furthermore, high-technology devices are replacing some of the security guard posts. Another factor that must be considered is the use of armed guards. Executive management usually does not want an armed guard presence, and some laws may prohibit their use. However, if you want to create a presence of serious security, there is nothing like an armed guard at the corporate lobby to give that impression. There are many

pros and cons of the use of armed guards. Because of the high value of some corporate assets, it may be deemed appropriate to have armed guards at some locations but not others. That presents the problem of who is placed in what guard positions and decreases the effective and efficient use of guards to fill any guard job within the corporation. In addition, the armed guards are more highly trained and may also press for higher pay for being armed. Their reasoning is that if they are armed, they are more trusted than those who are not armed, their job is more dangerous, and they are more highly skilled.

Alarms and Surveillance within the Inner Layer. The application of alarms and surveillance within the inner layer of security requires the same considerations as the application to the outer layer. The extent to which they are used or not used depends on threats, vulnerabilities, risks, and the criticality of assets within.

PHYSICAL SECURITY COSTS

The cost of physical security is always a concern. Reaching an appropriate balance between adequate protection levels and the cost of that physical protection is difficult. Too little security leaves vulnerabilities in place, increasing risks. Too much security mitigates threats and vulnerabilities and reduces risks but leads to unnecessary expenditures. Inefficient application of security controls (spending more than you need to for a physical security service or product) uses scarce resources that otherwise are available for additional protective measures. Objectively demonstrating to management the effectiveness of security controls is problematic. It is difficult to quantify the value of deterrence achieved through the application of physical protective measures.

A common security axiom is: The more doors and openings a building has, the more difficult it will be to control access. There is a trade-off here: the cost of security weighed against the convenience of employees and others. It all comes down to costs and what executive management considers acceptable risk levels.

PHYSICAL RISK ASSESSMENTS

The CSM knows that fundamental to developing an effective physical security profile is in part his or her understanding of the various threats to assets and the likelihood of an actual occurrence. Recognizing threats allows for cost-effective implementation of security measures. Implementing security measures that have little or no relationship to the type of threat associated may be an inefficient use of resources. Moreover, implementing redundant protective measures may not improve assets protection but will certainly consume resources better spent elsewhere.

Assessing the physical threats after identifying vulnerabilities is not easy. It requires an understanding of the business environment. One way to better assist the CSM in the effort to understand physical threats is through benchmarking. Identify businesses similar to yours and talk to them about their perceived threats. Try to find out what protective measures they implement to mitigate physical threats. There are other means of threat assessment:

- Consult experts in your line of business
- Seek the guidance of security professionals in similar situations
- Consult with your insurance provider
- Talk to risk managers
- Talk to the local police about crime in your area

Risk assessment is the product of determining the threats and understanding their consequences. If the consequences are significant, protective measures should be implemented. If the consequences are not significant, implementing additional protective measures may be an inefficient use of resources and would not add value. Implementing physical security measures to the extent that all threats are eliminated is an action of risk avoidance. For some business, risk avoidance is appropriate. For most businesses it is not.

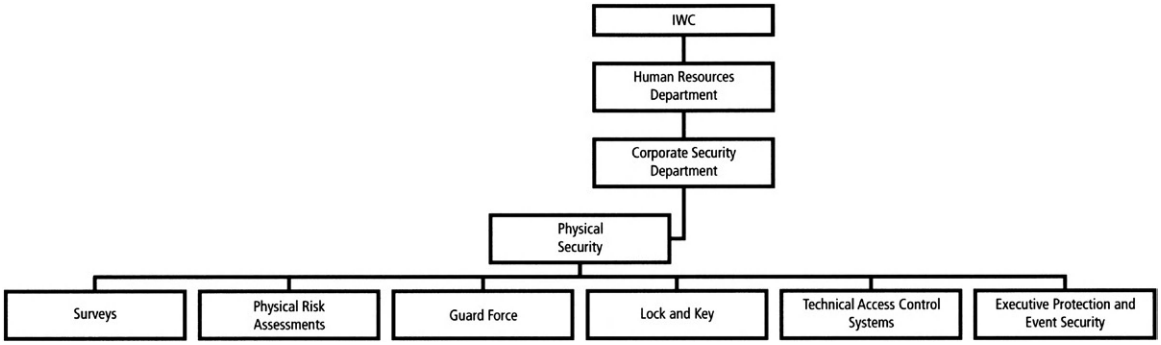


FIGURE 21-2 Basic assets protection measures.

PHYSICAL SECURITY FOR CLASSIFIED GOVERNMENT CONTRACTS

All of the physical controls mentioned in this chapter have applicability in some way to the physical security requirements of government contracts. However, for specific guidance, applicable government security publications and requirements documents (e.g., contracts) must be consulted.

In the United States, *The National Industrial Security Program Operating Manual* [1] is the basic document providing guidance for physical security. Special access programs and sensitive compartmentalized information activities generally have additional, very specific physical requirements addressing everything from construction specifications to locking devices. The applicable documentation must be consulted prior to planning construction for any area supporting these activities. The appropriate government-cognizant security officer must be consulted, since formal approval is generally required prior to use.

SUMMARY

The physical security function through a CSM's physical security organization is the foundation for basic assets protection measures (Figure 21-2). To this foundation, or baseline, additional controls for protection of assets are added, creating a complete protection profile. No single physical security control can satisfy all of the assets protection needs.

Physical security is built in layers. Each layer of security control serves a specific purpose by providing specific protections. Many controls used in conjunction with each other help to create a secure environment.

Conducting a site physical security survey should enable the gathering of all information necessary to make an intelligent and informed risk assessment of the sites or facilities and create a physical security profile. From this point, additional controls can be developed and implemented to provide the most cost-effective security profile tailored to the specific needs of an enterprise.

REFERENCE

[1] United States Department of Defense. The National Industrial Security Program Operating Manual (DoD 5220.22-M), available at http://www.dss.mil/isec/nispom.htm, January 1995. This manual was issued in accordance with the National Industrial Security Program as authorized by Executive Order 12829.

CHAPTER

22

Fiber Optics and Robots

Lawrence J. Fennelly, CPP, CSS, HLS III

This chapter discusses two topics: fiber optics and robots.

FIBER OPTICS

An *optical fiber* is a flexible, transparent fiber made of very pure glass (silica) not much bigger than a human hair that acts as a waveguide, or "light pipe," to transmit light between the two ends of the fiber [1]. The field of applied science and engineering concerned with the design and application of optical fibers is known as *fiber optics*. Optical fibers are widely used in fiber optic communication, which permits transmission over longer distances and at higher bandwidths (data rates) than other forms of communication. Fibers are used instead of metal wires because signals travel along them with less loss and are also immune to electromagnetic interference. Fibers are also used for illumination, and are wrapped in bundles so they can be used to carry images, thus allowing viewing in tight spaces. Specially designed fibers are used for a variety of other applications, including sensors and fiber lasers.

Optical fiber typically consists of a transparent core surrounded by a transparent cladding material with a lower index of refraction. Light is kept in the core by total internal reflection. This causes the fiber to act as a waveguide. Fibers that support many propagation paths or transverse modes are called multimode fibers (MMFs), while those that only support a single mode are called single-mode fibers (SMFs). Multimode fibers generally have a larger core diameter and are used for short-distance communication links and in applications where high power must be transmitted. Single-mode fibers are used for most communication links longer than 1,050 meters (3,440 ft).

Joining lengths of optical fiber is more complex than joining electrical wire or cable. The ends of the fibers must be carefully cleaved and then spliced together either mechanically or by fusing them with heat. Special optical fiber connectors for removable connections are also available [2].

Mary Lynn Garcia, in her book *Vulnerability Assessment of Physical Protection Systems*, stated that for "fiber optic cable used on interior walls, the cable detects cutting through the wall by checking sensor, generally used in high-security systems or close to valuable assets" (p. 116).

Fischer and Green stated in their book *Introduction to Security* that for installation of

> *fiber optic cable, a beam of pulsed light is transmitted through the cable, and this is sensed at the other end. If the cable is cut or interfered with, the pulsing stops and there are changes in amplitude. The application of the cable is similar to the electromagnetic cable. Some manufacturers of high-security fences, however, have incorporated the fiber optic cable into the hollow strand of their normal fence material, making it*

> *impossible to detect. The sensing cable may be attached to a fence, buried alongside a pipeline, or used in conjunction with power or communications lines. The use of fiber optic cable allows monitoring of miles of fence, pipe, or transmission lines with no electronics or power in the field. (p. 181)*

Geoff Craighead, in his book *High-Rise Security and Fire Line Safety*, 3rd edition, states

> *CCTV involves the transmission of scenes or moving pictures from a video source, such as a camera, by conversion of light rays to electronic signals, which are transmitted via coaxial cable, fiber-optic cable or twisted pair wire or by microwave links, infrared wireless transmission, radio frequency (RF) wireless transmission, telephone wires, networks and a host of other methods. (p. 321)*

Advantages of Fiber Optics [3]

Why are fiber optic systems revolutionizing telecommunications? Compared to conventional metal wire (copper wire), optical fibers are:

- **Less expensive.** Several miles of optical cable can be made cheaper than equivalent lengths of copper wire. This saves your provider (cable TV, Internet) and you money.
- **Thinner.** Optical fibers can be drawn to smaller diameters than copper wire.
- **Higher carrying capacity.** Because optical fibers are thinner than copper wires, more fibers can be bundled into a given-diameter cable than copper wires. This allows more phone lines to go over the same cable or more channels to come through the cable into your cable TV box.
- **Less signal degradation.** The loss of signal in optical fiber is less than in copper wire.
- **Light signals.** Unlike electrical signals in copper wires, light signals from one fiber do not interfere with those of other fibers in the same cable. This means clearer phone conversations or TV reception.
- **Low power.** Because signals in optical fibers degrade less, lower-power transmitters can be used instead of the high-voltage electrical transmitters needed for copper wires. Again, this saves your provider and you money.
- **Digital signals.** Optical fibers are ideally suited for carrying digital information, which is especially useful in computer networks.
- **Nonflammable.** Because no electricity is passed through optical fibers, there is no fire hazard.
- **Lightweight.** An optical cable weighs less than a comparable copper wire cable. Fiber optic cables take up less space in the ground.
- **Flexible.** Because fiber optics are so flexible and can transmit and receive light, they are used in many flexible digital cameras.

ROBOTS AS SECURITY DEVICES

Having robots supplement loss prevention personnel is not futuristic speculation: robotic technology is here today. These devices are capable of traveling around a facility to relay information back to a control center staffed by human beings. Some present-day robot characteristics are CCTV, lights, infrared sensors to detect movement, communications equipment that allows the human at the control center to speak through the robot, a piercing siren and bright light to stun an intruder, and an extinguisher to suppress a fire. The robot's greatest asset is that it can enter hazardous areas that would be dangerous to human beings. Consider that a robot can be used to confront an armed offender, or can be used during a nuclear accident, bomb threat, or fire. Robots can be replaced; humans cannot. Robots are also repairable, but humans suffer from injuries. The losses from the death of an employee are far greater than from a destroyed robot.

The use of robots will expand in the future, especially when they are mass produced at lower prices. The robots of tomorrow will be more sophisticated and better equipped. Perimeter patrol, access control, searching people and other robots, detaining offenders, analyzing loss vulnerabilities, and performing inspections and

audits will be standard jobs for robots. They will eventually outperform humans. Flying, carrying, and pulling huge loads, and the ability to see, hear, smell, taste, and touch with greater perception than humans are inevitable capabilities.

Lawsuits involving the liability of a robot's owner for, say, excessive force against an offender, will be common. Humans must be ready to "pull the plug" on a robot when necessary.

The International Foundation of Robotics (IFR) statistical department reported continuing growth of robot sales worldwide:

> *According to the results of the first quarter 2011 of the IFR Quarterly Statistics the robots sales increased by 53% compared to the first quarter 2010. In the fourth quarter 2010 the growth of robot sales slowed down somewhat. However, the level in all three regions—North America, Europe and Asia—rose compared to the fourth quarter 2010. Especially sales of robots for handling operations and welding increased above average.*[1]

SUMMARY

In summary, I leave you with a question: Would you consider the replacement of personnel who view CCTV monitors all day (24/7) with a proven-to-work-and-react robot?

REFERENCES

[1] International Foundation of Robotics, page 1.
[2] www.Wikipedia.com, Defining Characteristics, 2012.
[3] Freudenrich, C. How fiber optics work. Available at *www.stonewallcable.com.*, 2011.

INDEX

A

AAMA. *See* Architectural Manufacturers Association
AC&D. *See* Alarm communication and display
Access cards, 265–266
  biometric ID systems, locks to doors, 266
  biometrics access control, 266
  card readers, 266
  dual-technology card, 266
  EAC systems applications, 266
  proximity access cards, 265
  Smart cards, 266
  magnetic stripe cards, 265–266
  Weigand cards, 266
Access control, 257, 328
  on badges, 350–351
  on building lobbies and doors, 350
  by employees, 349
  on guards, 351–352
  on interior areas and rooms, 350
  in layers, 349
  by outsiders, 350
  tactical-environment considerations, 264–267
  on vehicle and personnel gates, 350
  by vehicles, 349
Access control interfaces, 318
Access control mechanized/automated systems, 260
Access control rosters, 263
Access verification workstations, 316
Administrative workstations, 316
Alarm assessment, 24
Alarm communication and display (AC&D), 25–26
Alarm control, 200
  batteries, 200
  logging, 200
  logout, 200
  microprocessors, 200
  sensing devices, 200
  tamper protection, 200
Alarm systems, 191–199
  area/space protection devices, 194
  components, 191–199
  door switches, 192
  equipment overhaul, 203
  false alarms, 199
  glass break detectors, 192
  interior sensors, 194
  lace and panels, 193
  perimeter protection devices, 191–194
  window screens, 193
  wooden screens, 192
Alarm transmission/signaling, 200–202
  central station system, 201–202
  total alarm, 201
Alarmed combination locks, 173–174
Alarms, 45
  for crime deterrence, 202
  and surveillance, within inner layer, 352
American National Standards Institute (ANSI)
  new standard for exit devices, 153
  standard for doors, 338
American Public Transportation Association, security-related guidelines, 288
American Society for Testing and Materials (ASTM), 273, 338
Analog camera with DSP and all-digital camera, block diagram, 222f
Analog CCTV camera, block diagram, 221f
Angel, Schlomo, 1
ANSI. *See* American National Standards Institute
Anticipation, 41
Appraisal, 41
Architectural Manufacturers Association (AAMA), 338
Area/space protection devices, 194
  carpets, furniture, and draperies, 194
  dual-technology sensor, 199
  grounding and shielding, 194
  interiors sensors, 199
  microwave, 194–198
  motion sensor survey, 195t–197t
  passive infrared motion detectors, 198
  photoelectric eyes (beams), 194
  pressure mats, 198
  sound sensors, 198–199
  types, 194
  ultrasonics, 194
  zoning, 199–200
ARPANET, 293–294
Artificial indoor illumination, 224–225
ASIS International, 228
Asociación Española de Normalización y Certificación (AENOR), 285
Association française de normalization (AFNOR), 285
ASTM. *See* American Society for Testing and Materials
Audit, 54–59
  exterior access controls, 54–55
  interior access controls, 55–56
  mail services security, 56
Auto theft prevention, 52–53
Automatic sprinklers, 279
  types, 279

B

Backhaul networks, 302–303
Badges, 266–267, 350–351
Ballast, 184
Benchmark (minimum) practices, 284
BHMA. *See* Builders' Hardware Manufacturer's Association
Bicycle registration and antitheft program, 52
Bill 168, 283–284
Biometric ID systems, locks to doors, 266
Biometrics, 255, 328
  behavioral biometrics, 255
  characteristics, 255–256
  devices, types of, 255–256
  physiological biometrices, 255
Biometrics access control, 266
Biting chart, 119
Brightness, 184
British Standards Institution (BSI), 285
Browser, 309–310
BSI. *See* British Standards Institution
Builders' Hardware Manufacturer's Association (BHMA), 153
  compliance for Dutch doors, 336
Building
  general purpose of, 44
  hazards involving, 44
Building grounds security strategies, 6
Building interior security strategies, 6
Building perimeter security strategies, 6
Bulbs. *See also* Lamps, 184, 188
Bullet-resistant doors, 75, 332
Bullet-resistant executive office products, 75, 332
Bullet-resistant fiberglass wall panels, 75, 332
Bullet-resistant glass, 94, 329
Bullet-resistant transaction or reception area, 75, 332
Bullet-resistant windows, 75, 332
Burglary, 191
Burglary-resistant files, 179

C

Cabling, 317
  fiber optic, 317
  multimode, 317
  single mode, 317
  wired cabling, 317
Camera, 310–312. *See also* Digital video camera.
  CCTV camera, 221f
  digital and progressive scan, 234–235
  functions of, 219–222
  LLL-intensified camera, 235
  monitor function, 221–222
  panoramic 360° lens, 236–237
  panoramic 360° lens, 230
  raster scanning, 234
  recording function. *See also* Security camera, 222
  scanning process, 232–235
  significant advancements, 232
  solid-state camera, 235
  thermal imaging camera, 235–236
  transmission function, 221
Camera capability vs. requirements, 224t
Camera housings, 246
  dome, 246
  plug and play, 246
  specialty, 246
  standard rectangular, 246

Note: Page numbers followed by "f" and "t" indicate figures and tables, respectively.

Canadian Standards Association (CSA), 284–285
Card control, 44
Card readers, 266
Cash off the streets strategies, 7
CCTV. *See* Closed-caption television
CCTV camera, regulatory considerations, 285–286
Chain-link fabric, 270–271
  gates, 271
Chain-link fencing, 269
  security planning, 269–270
    A-B-C-D method, 269–270
  chain-link fencing, 269
  design features, 271
  detail of, 275f
  framework, 270
  gates, 271
  installation, 273
  material specifications, 270–271
  project inspection, 273
  specifications, 272
Chain-Link Manufacturers Institute, 273
Chula Vista, 337
Circuit (party line) systems, 201
Citizen intervention, 7
Citizen patrols, 53
Citizen–police support strategies, 7
Client/server configuration, 307–308
Closed-circuit television (CCTV), 47, 79, 87
  in surveillance process, strengths and weaknesses, 345t
Closed-circuit television operators, 325–326
  digital video recorders, 326
  locations for, 327–328
  targets, 327
  schedule areas, 327–328
  testing and maintenance, 328
Coaxial cable, 238
Codec, 310
Coefficient of utilization, 184
Color rendition index (CRI), 183, 187
Combination locks, UL-rated, 170
Command center, 325–326
Compliance-based vulnerability approach, 33, 34t
Confidence restoration strategies, 7
Conklin, John, 2–3
Consequence analysis, 13
Construction Specifications Institute, 273
Construction standards strategies, 6
Contrast, 184
Control methods
  escorts, 263
  two-person rule, 263–264
Corporate security manager (CSM), 340
  responsibility of, 340
  risk assessment, 352
Covert pinhole lens, 230
CRI. *See* Color rendition index (CRI)
Crime analysis, 46
Crime prevention
  definition, 41
  physical, use of locks in. *See* Locks
Crime prevention through environmental design (CPTED), 9–10
  cautions, 5
  current projects
    cities, applications in, 8
    confidence restoration strategies, 7
    law enforcement strategies, 7
    personal defense strategies, 6–7
    school design, application to, 8
    territorial defense strategies, 6
  future of, 8–9
  publication, 10
Crime risk, 41–42
  reduction, initiation of action, 42
Cross keys, 123–124
CSA. *See* Canadian Standards Association
Custodians, 45
Customers, 350

D

Data collection
  delay
    active/passive barriers, 28
    adversary, 27
    concept in, 27
    times, estimation of, 27
  detection of
    alarm assessment, 24
    alarm communication and display (AC&D), 25–26
    entry control subsystem, 24–25
  intrusion sensor, 22–24
  response, 28–29
Day condition vs. night conditions, light levels, 223t
Dead bolt, 130f, 131–132
Dead bolt, 338
Defensible space
  architectural guidelines, 4–5
  definition, 2
  existing facilities, modification of, 5
  natural surveillance, 4
  territoriality, 3–4
Delayed action timers (DATs), 173
Department of Housing and Urban Development (HUD), 5–6
Design-reference threat, 82–86
Diffuser, 184
Digital biometrics signature, 256
Digital closed-circuit television (CCTV), 47
Digital communicators, 202
Digital image resolution, 312
  storage issues, 314
Digital scanning, 234–235
Digital video camera, 310–312. *See also* Camera.
  frame rates, 312
Direct wire systems, 201
Disc tumbler mechanisms, 119–120, 120f
Disk storage, 315
  network attached storage, 315
  operating systems and programs, 315
  storage area network, 315
  tape or disk, 315
Door switches, 192
Doors, 335–338
  functions, 337–338
  lock types
    cylinders, 133–136, 135f
    cylindrical lockset, 133, 134f
    mortise, 133, 134f
    padlocks, 136–138, 136f–137f
    rim-mounted mechanism, 133, 134f
    tubular, 133, 134f
    unit lock, 133, 134f
  mechanical locking devices, 337
  in residential buildings, 336–337
    exterior doors, 336–337
    exterior doors in commercial or business applications, 337
    mechanical locking devices, 337
    strike plates, 337
  standards for, 338
  terms and definition, 155–167
Double-hung wood, 331
Dual-split lenses, 230
Dual-technology card, 266
Duress code, 263
DVR, 245

E

EAC systems applications, 266
Electric strike, 338
Electrical power, 188
Electroluminescent lights, 183
Electronic vibration detector (EVD), 200
Emergency doors, 104–105, 106f
Employee screening, 258–259
Employees, 349
Enterprise LAN, 318
E155 and L156, "Building Design for Homeland Security", 287
Escorts, 263
European Committee for Electrotechnical Standardization (CENELEC), 285
Event and fault tree analyses, 13
Exterior doors, 336–337
  in commercial or business applications, 337

F

Facial recognition device, 255–256
Facilities Physical Security Measures, ASIS GDL, FPSM-2009, 10
False alarms, 199, 202–203
  motion, 194
  noise, 194
  radio or electrical interference, 194
Federal Emergency Management Agency (FEMA), 287
FEMA 389, "Communicating with Owners and Managers of New Buildings on Earthquake Risk", 287
FEMA 426, "Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings", 287
FEMA 427, "Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks", 288
FEMA 428, "Primer for Design Safe Schools Projects in Case of Terrorist Attacks", 288
FEMA 430, "Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks", 288
FEMA 452, "A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings", 287
FEMA 453, "Safe Rooms and Shelters—Protecting People Against Terrorist Attacks", 287
Fences, 342
Fencing. *See* Chain-link fencing
FFL lens. *See* Fixed-focal length (FFL) lens
Fiber optics, 355. *See also* Optical fibers.
  advantages, 356

Field Inspection Guide, CLFMI, 273
Finger reader recognition systems, 255
Fingerprints, 255
Fire safety inspection, 279
  administrative and planning phase, 279–280
  alarm system inspection phase, 281–282
  extinguisher inspection phase, 280–281
  general physical inspection phase, 280
  hazardous materials inspection phase, 281
  sprinkler system inspection phase, 281
  stand pipe, fire hose, and control valve inspection phase, 281
Fire-resistant containers, 179, 180t
Firewalls, 301
Fixed-focal length (FFL) lens, 219, 228–229
  and their FOVs, 228f
Fixture. *See also* Luminary, 184, 188
Flag hinge, 338
Float glass/annealed glass, 329
Fluorescent lamps, 182, 184–185
Foot-candle, 184
Foot-lambert, 184

G
Gates, 342–343
GionGreen, 179
Glare, 184
Glass, types of, 329
Glass break detectors, 192
Gravity tanks, 279
Guard or lobby desk workstations, 316
Guards, 351–352
  in surveillance process, strengths and weaknesses, 345t

H
Halogen lamps, 182
Hand scanner, 255
Hard-copy video printers, 245–246
  ancillary equipment, 246–249
  camera housings, 246
  camera video annotation, 249
  image reversal, 249
  pan/tilt mounts, 246–248
  screen splitter, 248–249
  VMD, 248
Hardened doors, 98f–100f, 99, 100
Hardware configurations, 315
  CPUs, 315
  memory, 315
Hard-wired transmission video signal
  coaxial cable, 238
  UTP, 238
HID. *See* High-intensity discharge
HID lamps, 185
High-intensity discharge (HID), 184
High-pressure sodium lamps, 182
High-Rise Security and Fire Line Safety (Craighead), 356
Hollow-core door, 335
Home security checklist, 70
  basement doors and windows, 52
  entrances, 51–54
  garage and basement entrances, 52
  garage doors and windows, 52
  ground floor windows, 52
  protecting personal property, 52–54
  upper floor windows, 52
Hubs, 300
Human eye and video camera, comparison of, 219f

I
ID methods, 259
  card-/badge-exchange system, 259
  multiple-card/-badge system, 259
  personal-recognition system, 259
  sign/countersign and code word, 263
  single-card/-badge system, 259
Identification system, 259
Illicit keys, 140
Illuminance, 182
Illuminare, 184
Image reversal, 249
Incandescent lamps, 182, 184
Inner layers, of physical security, 346–349
  areas, 348–349
  buildings, 347
  doors, 347
  glass, 347
  locks and keys, 347–348
  roofs, 348
  rooms, 348–349
  safes, 349
Institute of Electrical and Electronics Engineers, 298
Intelligence
  vs. object size, 226f
  vs. TV lines, 226t
Interfacing
  enterprise LAN, 318
  process control networks, 318–320
  wide area network, 318
Interior areas and rooms, 350
Interior sensors, 194
International Council on Systems Engineering (INCOSE), 33
International Foundation of Robotics (IFR), 357
International Organization for Standardization, 284–285
  adoption, 285
  employing licensed personnel, 286
  implementation, 284
  managing compliance, 289–291
  national standards bodies, 284–285
  physical and information security, 286
  regulatory considerations, 285–286
International Standards Organization (ISO), 338
Internet, 238
Intranet, 238
Introduction to Security (Fischer and Green), 355
Intrusion alarms, 47–48
Intrusion detection systems, 301
Investor confidence strategies, 7
Iris cameras, 255
Iris recognition, 255

J
Jeffrey, C. Ray, 3
JPEG resolution, 312

K
Key control, 44
Key-operated mechanism
  change key, 117–118
  code of, 118
  combinations availability, 118–119
  depth intervals, 118, 118f
  disc or wafer, 119–120, 120f
  key cut, spacing/position of, 118, 118f
  lever, 125–128, 125f–127f
  pin tumbler mechanism. *See* Pin tumbler mechanisms
Kick-off meetings, 20–21
Kleenex™, 296

L
Lace and panels, 193
Laminated glass, 329
Lamps. *See also* Bulbs, 184, 188
LAN, 238
Land-use planning strategy, 6
Latch bolt, 130–131, 130f–131f
Law enforcement strategies, 7
LCD high-resolution screen, 312
LED (light-emitting diodes), 183
Lens, 184
  covert pinhole lens, 230
  dual-split and tri-split lenses, 230
  FFL lens, 228–229
  panoramic 360° lens, 230
  varifocal lens, 229–230
  zoom lens, 229
Leudtke, Gerald, 2
Lever tumbler mechanisms, 125–128, 125f–127f
Levers, 338
Lewis Technology, 294
Licensing
  of the installer, 286
  of camera operator, 286
Light-gauge residential chain-link fabric, 270
Lighting, 344
  checklist, 186
  deficiency, 181
  definitions
    components, 188
    corrected color temperature (CCT), 188
    CRI, 187
    lumens, 187
    reflectance, 187
  description, 188
  energy management, 185–187
  illumination, 182
  lamps, types of
    color rendition index, 183
    cost and ROI, 183
    lighting equipment, 183–184
    outdoors application, 182
  levels, 181, 187
  objectives, 184–185
  operation costs, 189t
  protective lighting checklist, 186–187
  purposes of, 181
  sources, 183
  types, 188t
  and security, 48
    streetlights, 48
Lighting equipment, 183–184
Lobbies and doors, building of, 350
Local law enforcement authorities (LLEA), 81

Locks, 44
attack and countermeasures
on bolts, 147–149, 148f–149f
on cylinders, 149–151, 150f–151f
key security, 140–141
manipulation, 141–146, 143f–144f
shimming, 146–147
surreptitious attacks, 140
bodies
dead bolt, 130f, 131–132
latch bolt, 130–131, 130f–131f
combination, 128–129, 128f
doors and windows security, terms and definition, 155–167
door type
cylinders, 133–136, 135f
cylindrical lockset, 133, 134f
mortise, 133, 134f
padlocks, 136–138, 136f–137f
rim-mounted mechanism, 133, 134f
tubular, 133, 134f
unit lock, 133, 134f
exit alarms and exit, 153
key control system, 152
key-operated mechanism. *See* Key-operated mechanism
security checklist, 154–155
and security systems, 151–152
strikes, 138–139, 139f
terminology and components, 117
Locks and keys, 347–348
Louvers, 184
Low-light level (LLL)-intensified camera, 235
Low-pressure sodium lamps, 182
Lumens, 182, 184, 187
Luminaire, 184
Luminary. *See also* Fixture, 188
Lux, 184
Lystad, E., 2

M
Magnetic stripe cards, 265–266
Mandatory practices, 283–284
Massachusetts Crime Watch, 51
basement doors and windows, 52
entrances, 43
garage and basement, 52
garage doors and windows, 44
ground floor windows, 52
protecting personal property, 52
upper floor and windows, 52
Master keys, 123–124, 124f, 153
Master pins, 123–124, 124f, 163
Master sleeve, 124
Maximum security
characterization, 79
concept of, 77, 80–81
design, 81
perimeter alarm system, 87
psychology of, 80–81
security, highest level of, 78f, 80
Mechanical locking devices, 337
Mechanized/automated systems, 260
Mercury vapor lamps, 182
Metal halide lamps, 182
Mini-pinhole lenses, 231f
Monitors
audio/video, 244
color, 243
CRT, 243–244
LCD, 243–244
monochrome, 242–243
plasma, 243–244
Monochrome cameras, 222
Mortice lock, 338
Motion effect, 227
Mounting hardware, 188
MPEG resolution, 312
Multicamera video security system, 214–215
ancillary supporting equipment, 215
annotator, 216
dome housing, 215
housings, 215
pan/tilt mechanism, 216
plug and play camera/housing combination, 215–216
splitter/combiner/inserter, 216
Multimode fibers (MMFs), 355
Multiple-card/-badge system, 259
Multiplex systems, 202

N
National Association of Architectural Metal Manufacturers (NAAMM), 338
National Burglary and Fire Alarm Association (NBFAA), 203
National Crime Prevention Institute, 202
Natural barriers, 343
definition, 93
functions of, 95
Neighborhood identity strategies, 7
Neighborhood watch, 53
Nerve plate, 171–172
glass nerve plates, 172
Network architecture, 302–307
backhaul networks, 302–303
simple networks, 302
subnets, 303–306
VLANs, 306–307
Network communications speeds, 317
Network configurations, 307–308
client/server configuration, 307–308
peer-to-peer network, 307
Network infrastructure devices
firewalls, 301
hubs, 300
intrusion detection systems, 301
routers, 301
switches, 300
Networked digital video system, block diagram, 216f
Newman, Oscar, 2
NFPA 101, 2009, 338
NFPA 80, 2007, 338
North American Security Products Organization (NASPO), 285
NRC Canada test series, average alarm time for, 278t
Nuclear Regulatory Commission, 283

O
Object/spot detection, 200
capacitance/proximity detectors, 200
vibration detectors, 200
Obscuration detectors, 278–279
Occupational Health and Safety Act (OHSA), 283–284
One-camera system, 214f
camera, 214
hard-copy printer, 214
lens, 214
monitor, 214
recorder, 214
transmittal link, 214
Open Systems Interconnection (OSI), 294
Operation identification, 52
Optical disk, 245
Optical fibers, 355–356
advantages, 356
joining lengths, 355
OSI layers, 294f
Österreichisches Normungsinstitut (ON, Austrian Standards Institute), 285
Ostrich syndrome, 81
Outer layer, of physical security
alarms, 345–346
buildings, 343
doors, 343
fences, 342
gates, 342–343
grounds, 341
lighting, 344
natural barriers, 343
parking, 343–344
perimeter protection, 342–343
roads, 341–342
surveillance, 345
walls, 342

P
Padlocks, 136–138, 136f–137f
Panoramic 360° lens, 230f, 236–237, 236f
Panoramic 360° lens, 230
Parking, 343–344
PEBX interface, 318–319
People strategies, safe streets for, 7
Performance-based vulnerability approach, 33, 34t
Perimeter protection, 191–194
Personal defense strategies, 6–7
Personal-recognition system, 259
Personnel doors
existing security-class door, 100, 100f
hardened door, 99, 99f
hollow steel, 98, 98f
penetration resistance, 99
Photo ID workstations, 316
Physical barriers
access controls, 87
alarm systems, 87
CCTV, 87
communications, 87
concept of, 97
doors
countermeasures, 101
emergency, 104–105, 106f
existing, retrofit upgrading of, 100–101
frame interlocking, 101–102
frames, 101
function, 98
hardened, 98f–100f, 99–100
hinge vulnerability, 101
hollow steel door, 98–99
strong room, 104
vault, 103–104
vehicle, 102–103, 102t
weight, 102–105

entry and exit points, 86
bridle, 112–113, 112f
double-leaf swing gate, 113, 113f
fence gate locks, 112–113
turnstile gates, 112
vehicular gates, 112
fences
barbed-tape-topping, 111–112
bottom fence rail, 111, 111f
climb-over time, 110–111
cut-through time, 112
environmental conditions, 110
objectives, 109
penetration aids, 109, 110t
type of, 110
uses, 109
V-fence, 110
floors
construction, 108
I-beam application, 109, 109f
penetration resistance, 109
penetration time, 108–109
lighting, 87
LLEA coordination, 88
locks, 87
moats, 113–115
objective, 86
response force, 87
roofs
construction, 107
disassemble, 107
grappling hook shielding, 108, 108f
upgrading existing, 107–108
security force, 87
topography, 114–115
walls, 113–115
Physical design
and informal social control, relationship between, 1
urban residential complexes
CPTED. *See* Crime prevention through environmental design
defensible space. *See* Defensible space
Physical protection system (PPS)
evaluation process, 18f
vulnerability assessment. *See* Vulnerability assessment (VA)
Physical recommendation, 44
Physical risk assessments, 352
Physical security
for classified government contracts, 353
controlling access, 349–352
costs, 352
definition of, 339–340
fundamental principles, 339
in layers, 340
inner layers, 346–349
levels of, 77, 78f
high-level security, 79
low-level security, 78–79
maximum security, 79–81
medium security, 79
minimum security, 78
outer layers, 340–346
physical risk assessments, 352
planning, value of
components, 81, 82t
design-reference threat, 82–86
layering, 86, 86f
Pin tumbler mechanisms
cylinder, 122, 124f
depth intervals, 121
master-keyed, 123–125, 124f
modification, 122, 123
operation, 120, 122f
paracentric keys, 121–122, 123f
removable core, 122–123, 124f
structure, 120, 121f
warded keyways, 121–122, 123f
Pinhole lenses, 231f
Police officer applications, 44
Police patrol strategies, 7
Post orders, 325
PPS. *See* Physical protection system
PPS process, evaluation, 18f
Probability of neutralization, 14
Process control networks, 318–320
access control interfaces, 318
building automation systems, 318
elevators/shifts, 318
fire alarm systems, 319
parking control systems, 320
PEBX interface, 318–319
public address systems, 319–320
vending access management systems, 320
voiceover IP systems, 319
Progressive scanning, 234–235
Project management, 19–20
Protective barriers
establishment, 93
fence
security, type of, 96
standard, 96
natural, 93
perimeter entrances
active structural barriers, 95
entry-control stations, 94–95
internal barriers, 95
passive structural barriers, 95
planning, 95–96
structural, 93
Proximity access cards, 265
Punching, 176

Q

Qualitative and quantitative analysis approaches, application, 15f
Quantitative analysis, in vulnerability assessment, 16–18
Quartz halogen lamps, 182
Quartz lamps, 183

R

Radio signal transmission, 202
Rainwater, Lee, 1
Rand, George, 2
Raster scanning, 234
Reception area, 332
Recognition, 41
Recorders
DVR, 245
optical disk, 245
VCR, 244–245
Reflectance, 187
Reflectivity, 226–227
of common materials, 227t
Reflector, 184
Relocking devices, 171–172
Reppetto, 2
Residential high-level security, for corporate executives, 332
Residential security, 49–51
alarms, 51
defensive measures, 49
entrances, 50
inner defenses, setting up, 50–51
lighting, 51
windows, 49–50, 50f
Restricted areas, 257
Rim lock, 338
Ripping or chopping, 177
Robots
lawsuits, 357
as security devices, 356–357
use of, 356–357
Roofs
construction, 107
disassemble, 107
grappling hook shielding, 108, 108f
upgrading existing, 107–108
Routers, 301

S

Safes, 179
burglaries, 175
buyers, 174
carting off, 177
dealers, 174
fire-resistant, 169
locking, fully scramble during, 176
opening problems, overcoming, 177–179
peeling, 176–177
protective rings, 169
punching, 176
rating, 179–180
ripping or chopping, 177
skilled attacks, 177
UL labeling, 169
writing combination, 175–177
Safety, definition, 12
Sarbanes-Oxley Act 2002, 290
Scene characteristics
effects of motion, 227
reflectivity, 226–227
scene temperature, 227
target size, 226
Scene illumination, 222–225
artificial light, 224–225
natural light, 223–224
Scene temperature, 227
Schedule card/badge
access control, 262–263
enforcement measures, 262–263
specifications, 260
Security
audit. *See* Security audit
community reaction, 46
complex, personality of, 45
concerned points, 44–45
conducting survey
reasons to, 42
time for, 42
crime analysis, 46
definition, 12
digital closed-circuit television, 47
home security checklist. *See* Home security checklist
intrusion alarms, 47–48
key control, 46–47

Security *(Continued)*
lighting and, 48
negative aspect, 45–46
office checklist, 69–70
officers checklist, 68–69
other aspects, 48
physical. *See also* Physical barriers, 61
plant security checklist, 65–67
points, development of
dos and don'ts, 43–44
other effective surveyor, 44
positive aspects, 45
residential. *See* Residential security
risk analysis, 42
site survey and risk assessment, 59–61
survey follow-up, 49
survey recommendation, classification of
maximum security, 42–43
medium security, 43
minimum security, 43
surveyor, components for, 41
threats, 54
window film, 76
workplace, bullet-resistant glazing for, 74–75
Security and control
access control, 257–258
considerations, 258
degrees of, 257–258
layered levels, 265
package-control system, 264
Security audit, 54
access control and badge designs, 57
badges, 56–57
emergency planning, 57–58
emergency response, 58–59
exterior access controls, 54–55
fire and life safety, 59, 71
incidents, reporting of, 58
interior access controls, 55–56
investigations, 58
lock and key controls, 56–57
mail services security, 56
search policy, 57
Security camera, 232
Security command workstations, 316
Security container
alarmed combination locks, 173–174
lockable blot, 172
locking combination dials, 172
relocking devices, 171–172
safe. *See* Safes
selection of, 179
time-delay locks, 173
time locks, 172–173
UL-rated combination locks, 170
Security industry license, 286
Security officer
areas to train, 325
CCTV for, 327–328
designated restricted areas, 328
and equipment monitoring, 325–328
fixed cameras, 326
post order, 325
PTZ camera, 326
tasks, 326
timing, 326
Security officer applications, 44
Security plan
approach
formulation of, 90
presenting of, 90
justification
company's experience, 89
mental evaluation, 89
personal experience, 89
process, 90, 90f
steps, 89
Security risk, equation for, 14
Security surveys, 53
follow-up, 49
Security system digital networks
communications media, 297–300
edge devices, 297
single-mode fiber, 315
Sensing devices, 191
Servers process, 301–302, 314
archive service, 301
broadcast service, 301
directory service server, 301
e-mail service, 301
FTP or HTTP service, 301
mass storage, 302
printers, 302
program service, 301
workstations, 301–302
Sheet glass, 329
Shielded dials, 174
Shimming, 146–147
Simple networks, 302
Single-card/-badge system, 259
card-/badge-exchange system, 259
Single-mode fibers (SMFs), 355
Site design, 4
Site interrelationships design, 4
Site, facility, and building, layers within, 341f
Smart cards, 256, 266
SMFs. *See* Single-mode fibers
Solid-core door, 335
Solid-state camera, 235
analog, 235
digital, 235
Internet service provider, 235
Spyproof dial, 174
Stages of fire, 277
automatic sprinklers, 279
classifications, 277–278
fire spreads, 277
gravity tanks, 279
UL Standard 217, 278–279
ways to put out fires, 277
Stand pipe, 279
Standardization Documents Order Desk, 273
Statistical analysis, in vulnerability assessment, 16–18
Steel Door Institute (SDI), 338
Steel-sheathed door, 335
Storage, 45
Storage area network, 315
Street design, 4
Streetlights, 48
Strike plates, 337
Strikes, 138–139
Strong room doors, 104
Structural barriers
active, 95
definition, 93
functions of, 95
passive, 95
Subnets, 303–306
limit network traffic, 304
segregate network traffic, 304–306
Suction tanks, 279
Suppliers, 350
Surveillance, 345
within inner layer, 352
strength and weakness of CCTV and guards, 345
Surveillance-specific design, 4
Switchers, 240
large security systems, 241
microprocessor controlled, 240–241
standard, 240
Switches, 300
System architecture, 314–318
archiving data, 315
cabling, 317
directory service, 314–315
disk storage, 315
edge devices, 316
firewalls, 317
infrastructure devices, 316
network communications speeds, 317
remote access services, 315
routers, 317
servers, 314
switches, 316–317
wireless nodes, 317
work stations, 316
Systems engineering process, 32f

T

Tactical-environment considerations, 264–267
access cards, 265–266
building design, 265
security, layered levels of, 265
Task or work lighting, 184
TCP/UDP/RTP, 295–296
Telephone dialer, 202
Tempered glass, 329
Territorial defense strategies, 6
Thermal detectors, 278–279
Thermal imaging camera, 235–236
Thermal monochrome video printer and hard copy, 244f
Threat analysis, 13
Thumb-turn cylinder, 338
Time locks, 172–173
Time-delay locks, 173
Topography, 114–115
Total security solutions, 331
Transport Control Protocol/Internet Protocol (TCP/IP)
address schemes, 297
cameras and codecs, 310–312
creating network efficiencies, 308–310
digital resolution, 312
display parity, 312–314
encapsulation, 295
fiber optic, 298
fixing bad communications, 295
interfacing, 318–322
of layering communications, 294–295
multicasting, 321–322
network architecture, 302–307
network configurations, 307–308

purpose of, 293–294
servers process, 301–302
signal communications, 293–295
system architecture, 314–318
User Datagram Protocol, 296–297
wired and wireless digital security systems, 320
Transportation strategies, 7
Trespassing, 45
Tri-split lenses, 230
Two-person rule, 263–264

U
UL Standard 217, 278–279
Underwriters Laboratories (UL), 51, 120
combination locks, 170
fire and burglary protection, 169
ratings for, 169
Underwriters Laboratory 305, 338
Uniform lighting, 184
User Datagram Protocol, 296–297
streaming data, 296
Unshielded twisted-pair (UTP), 214, 238

V
Varifocal lens, 229–230
Vault doors, 103–104
VCR, 244–245
Vehicles, 349
and personal gates, 350
Veiling reflection, 184
Vein recognition, 256
Vendors, 350
Very important persons (VIPs), 261
Video cameras, types of, 223f
Video lenses, types of, 220f
Video security technology, 213
advantages, 213
ancillary equipment, 246–249
camera function, 219–222
hard-copy video printers, 245–246
lenses, 228–232
monitors, 242–244
primary function, 213
quads and multiplexers, 241–242
recorders, 244–245
scene characteristics, 225–227
scene illumination, 222–225
switchers, 240
transmission, 237–240
video system, 216–219
Video signal transmission, 237–240
hard-wired, 238
Internet, evolution of, 238
Intranet, evolution of, 238
LAN, evolution of, 238
optical fiber, 239–240
WAN, evolution of, 238
wireless, 238–239
Video system
lens function, 218–219
light and reflection, role of, 217–218
Video verification, 202
Virtual private network (VPN), 310
Vision-restricting dials, 174
Visitors, 261, 350
civilians under government contract, 261
cleaning terms, 261–262
defense employees, 262
identification and control personnel, 260–261
very important persons, 261
VLANs, 306–307
Voice recognition voiceprint, 256
Voiceover IP systems, 319
Vulnerability analysis, 13
Vulnerability assessment (VA)
baseline analysis, 31
compliance-based analysis, 30
data collection. *See* Data collection
facility characterization, 21–22
performance-based analysis
PPS element, evaluation of, 30
qualitative or quantitative techniques, 30
planning of
kick-off meetings, 20–21
project management, 19–20
team establishment, 20
process, 11, 18–19, 18f
protection objectives, 21–22
quantitative analysis, 16–18
reporting and using
format, 31
goal of, 31
upgrade design, approaches to, 31–32
risk assessment and. *See* Vulnerability assessment and risk assessment
risk management and. *See* Vulnerability assessment and risk management
scenario analysis, 30–31
statistical analysis, 16–18
system engineering and. *See* Vulnerability assessment and system engineering
uses, 11
Vulnerability assessment and risk assessment
attack, probability of, 15–16
definition, 13–14
probability, 14
qualitatively or quantitatively measurement, 13–15
Vulnerability assessment and risk management
avoidance, 12
definition, 12–13
distribution of, 12
relationship between, 12, 13f
security, 12–13
Vulnerability assessment and system engineering
compliance- vs. performance based approach, 33
definition, 32
design and analysis, 36–38
design implementation, 33
domain, 33
installation and test, 38
performance-based approach, 33
process, 32–33, 32f
replacement, 38
requirements, 34–36
Vulnerability Assessment of Physical Protection Systems (Garcia), 355
Vulnerability assessment team, 20

W
Wafer tumbler mechanisms, 119–120, 120f
Walls, 342
WAN, 238
Watts, 184
Weigand cards, 266
Wide area network, 318
Window
selection of, 330
types and size of, 329–330
Window film, 333
Window screens, 193
Windows ironmongery, 331
Wireless nodes, 317
Wood, Elizabeth, 1
Wooden screens, 192
Workstation, 316

X
Xerox™, 296

Z
Zoom lens, 229
horizontal FOV, 229f